Universidade Federal de Santa Catarina

Departamento de Matemática

Curso de Licenciatura em Matemática

Uma Introdução aos Anéis Principais e Fatoriais

por

Dheleon de Barcellos Mendes

Florianópolis, julho de 2005.

Esta Monografia foi julgada adequada como TRABALHO DE CONCLUSÃO DE CURSO no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº15/CCM/05.

Professora da disciplina:

Carmem Suzane Comitre Gimenez

Professora Orientadora:

Virgínia Silva Rodrigues

Banca Examinadora:

Profª Albertina Zatelli

Profª Carmem Suzane Comitre Gimenez

Profª Giselle Spindler

Data da Defesa: 01 de julho de 2005.

Agradecimentos

À Deus.

Às professoras da banca que disponibilizaram-se a ler este trabalho.

À professora Albertina Zatelli que iniciou a orientação deste trabalho sempre com muita dedicação, contribuindo em muito no resultado alcançado. Acima de tudo, a professora mostrou ser uma grande pessoa.

À professora Carmem, que nos momentos em que foi preciso, mostrou empenho em ajudar.

Especialmente a professora Virgínia por seu empenho e responsabilidade na orientação deste trabalho, seu apoio e palavras de incentivo. Objetiva, precisa e atenciosa tentarei guardar seus ensinamentos. Valeu!

Ao professor Rubens Starke que com sua humildade e vontade de ensinar será sempre uma referência.

Agradeço também a todas as pessoas que de uma forma ou de outra estiveram presentes durante o curso, professores, funcionários e colegas. Em especial aos amigos Ismael, Sandro e Raphael e as amigas Thaíse, Kellen e Madeline.

Aos companheiros de moradia Moisés, Thiago, João, Marcelo, Rafael e Marcos.

À minha namorada Edilane pelo apoio e compreensão.

À minha família, especialmente aos meus pais Paulo e Bete, à Dina minha segunda mãe e ao meu irmão Dirceu, pelo incentivo em todos os momentos.

Índice

Introdução

A Teoria de Anéis é uma área de importância fundamental em álgebra. A mesma está totalmente conectada com outras grandes áreas como por exemplo, Teoria de Módulos, Teoria de Grupos (Anéis de grupos), Análise Funcional (Álgebra de operadores), etc.

Nosso objetivo nesse trabalho é estudar alguns anéis especiais, a saber anéis principais e anéis fatoriais, ambos são domínios de integridade (anéis comutativos, com unidade e sem divisores de zero). Nesse estudo, introduzimos os anéis quadráticos que são muito usados para encontrar alguns tipos especiais de exemplos, motivo principal para estudá-los.

No que segue, apresentamos uma disposição geral de nosso trabalho.

No capítulo 1, são apresentados os pré-requisitos necessários. Estudamos anéis, subanéis e ideais onde apresentamos vários exemplos.

No capítulo 2, somos mais específicos pois estudamos divisibilidade num domínio de integridade $\mathbb{A}$, conseqüentemente definimos máximo divisor comum e outras definições importantes como elementos irredutíveis e primos em $\mathbb{A}$. Apresentamos também vários exemplos usando anéis quadráticos, onde temos uma seção dedicada a eles. Esta pretende mostrar que os mesmos, embora domínios de integridade, mostram-se como anéis onde pode não existir máximo divisor comum entre dois de seus elementos.

Dentre estes anéis, citamos o anel dos inteiros de Gauss, $\mathbb{Z}[\sqrt{-1}\ ] = \{a+bi : a, b \in \mathbb{Z}\}$. Nesse anel, por exemplo, 5 não é primo pois é decomponível no produto de irredutíveis $1 + 2\sqrt{-1}$ e $1 - 2\sqrt{-1}$. Abaixo escrevemos um

pouco sobre Gauss.

"... Carl Friedrich Gauss (1777-1855) foi um menino prodígio. Gauss quando criança se divertia com cálculos matemáticos; uma anedota referente a seus começos é característica. Um dia, para ocupar a classe, o professor mandou que os alunos somassem todos os números de um a cem, com instruções para que cada um colocasse sua ardósia sobre a mesa logo que completasse a tarefa. Quase, imediatamente, Gauss colocou sua ardósia sobre a mesa dizendo: "Aí está!" O professor olhou-o com desdém enquanto os outros trabalhavam diligentemente. Quando o instrutor finalmente olhou os resultados, a ardósia de Gauss era a única com a resposta correta, 5050, sem outro cálculo.

O menino de dez anos evidentemente calculava mentalmente a soma da progressão aritmética $1 + 2 + \cdots + 99 + 100$, presumidamente pela fórmula $\frac{m(m+1)}{2}$ ..." ([6], pág. 343).

No capítulo 3, seguem os anéis principais e fatoriais com seus principais resultados. Exibimos alguns exemplos dos mesmos. Vemos nesta seção que os anéis principais são fatoriais e embora a recíproca não seja verdadeira, deixamos para exibir exemplos que mostram este fato no capítulo 4. Finalizamos, mostrando um anel que não é fatorial.

O capítulo 4 tem por objetivo apresentar uma aplicação dos anéis fatoriais e ao mesmo tempo fornecer exemplos que mostram que anéis fatoriais podem não ser anéis principais, como dissemos acima. Apresentamos as principais propriedades e resultados necessários ao desenvolvimento do capítulo, cujo principal resultado diz que se $\mathbb{A}$ é fatorial então $\mathbb{A}[x]$ também o é.

Capítulo 1

Pré-Requisitos

Neste capítulo apresentamos definições e resultados que são usados nos capítulos posteriores, permitindo assim um melhor entendimento do trabalho.

1.1 Anéis

Seja $\mathbb{A}$ um conjunto não-vazio onde estejam definidas duas operações, as quais chamamos de soma e produto em $\mathbb{A}$ e denotamos por $+$ e $\cdot$, respectivamente. Assim,

$$\begin{array}{rccc} + : & \mathbb{A}\times\mathbb{A} & \to & \mathbb{A} \\ & (x,y) & \mapsto & x+y \end{array} \quad \text{e} \quad \begin{array}{rccc} \cdot : & \mathbb{A}\times\mathbb{A} & \to & \mathbb{A} \\ & (x,y) & \mapsto & x\cdot y \end{array}$$

Chamamos $(\mathbb{A}, +, \cdot)$ ou simplesmente $\mathbb{A}$ um anel se as seguintes propriedades são verificadas para quaisquer elementos $x, y, z \in \mathbb{A}$:
(i) Associatividade da soma: $(x + y) + z = x + (y + z)$;
(ii) Comutatividade da soma: $x + y = y + x$;
(iii) Existência do elemento neutro: existe $0 \in \mathbb{A}$ tal que $0 + x = x = x + 0$;
(iv) Existência do elemento oposto: para todo x existe um único elemento $y \in \mathbb{A}$, denotado por $y = -x$, tal que $x + y = y + x = 0$;
(v) Associatividade do produto: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
(vi) Distributividade à esquerda e à direita do produto em relação à soma:

$$\begin{cases} x \cdot (y+z) = x \cdot y + x \cdot z \\ (x+y) \cdot z = x \cdot z + y \cdot z. \end{cases}$$

Se o anel $\mathbb{A}$ satisfaz a propriedade:

(vii) Existe $1 \in \mathbb{A}$ tal que $x \cdot 1 = 1 \cdot x = x$, para todo $x \in \mathbb{A}$, então $\mathbb{A}$ é dito um anel com unidade.

Se $\mathbb{A}$ satisfaz a propriedade:

(viii) Para quaisquer $x, y \in \mathbb{A}$, $x \cdot y = y \cdot x$, então $\mathbb{A}$ é um anel comutativo.

Se $\mathbb{A}$ satisfaz a propriedade:

(ix) Para quaisquer $x, y \in \mathbb{A}$ tais que $x \cdot y = 0$ então $x = 0$ ou $y = 0$, dizemos que $\mathbb{A}$ é um anel sem divisores de zero.

Se $\mathbb{A}$ é um anel comutativo com unidade e sem divisores de zero, dizemos que $\mathbb{A}$ é um domínio de integridade.

Um corpo é um anel comutativo $\mathbb{A}$ com unidade e que satisfaz a propriedade:

(x) Para todo $x \in \mathbb{A}$, $x \neq 0$, existe $y \in \mathbb{A}$ tal que $x \cdot y = y \cdot x = 1$.

Esta propriedade diz que todo elemento não-nulo de um anel $\mathbb{A}$ possui inverso multiplicativo.

Para facilitar a escrita escrevemos xy para denotar $x \cdot y$.

Observação: Todo corpo é um domínio de integridade.

De fato, sejam $x, y \in \mathbb{A}$ tais que $xy = 0$. Suponhamos $y \neq 0$. Pela propriedade (x) existe $y' \in \mathbb{A}$ tal que $yy' = y'y = 1$.

Logo, $x = xyy' = 0y' = 0$ e portanto $\mathbb{A}$ é um domínio de integridade.

Exemplo 1.1. O conjunto $\mathbb{Z}$ dos números inteiros é um domínio de integridade. No entanto, $\mathbb{Z}$ não é um corpo, pois com exceção de -1 e 1, nenhum elemento não-nulo possui inverso multiplicativo.

Exemplo 1.2. Seja $\mathbb{R}$ o conjunto dos números reais e $\mathbb{A} = \Im(\mathbb{R})$ o conjunto de todas as funções $f : \mathbb{R} \to \mathbb{R}$. Definimos duas operações no conjunto $\mathbb{A}$ do seguinte modo:

$$\begin{array}{rccc} + : & \mathbb{A} \times \mathbb{A} & \to & \mathbb{A} \\ & (f, g) & \mapsto & f + g \end{array} \qquad \text{e} \qquad \begin{array}{rccc} \cdot : & \mathbb{A} \times \mathbb{A} & \to & \mathbb{A} \\ & (f, g) & \mapsto & fg \end{array}$$

onde $(f+g)(x) = f(x) + g(x)$, $\forall\ x \in \mathbb{R}$ e $(fg)(x) = f(x)g(x)$, $\forall\ x \in \mathbb{R}$.

O conjunto $\mathbb{A}$ com as operações acima é um anel comutativo. Observe que a função constante zero é o elemento neutro (em relação a adição) e a função constante 1 é o elemento unidade. Provamos que $\mathbb{A}$ não é um domínio de integridade.

De fato, consideramos $f, g : \mathbb{R} \to \mathbb{R}$ definidas por:

$$f(x) = \begin{cases} 0 & \text{se } x < 0 \\ x & \text{se } x \geq 0 \end{cases} \quad \text{e} \quad g(x) = \begin{cases} x^2 & \text{se } x < 0 \\ 0 & \text{se } x \geq 0 \end{cases}$$

Vemos facilmente que $f(x)g(x) = 0$, $\forall\ x \in \mathbb{R}$ e portanto fg é a função constante zero. Logo, $\mathbb{A}$ não é domínio de integridade.

Exemplo 1.3. Consideramos $\mathbb{C}$ o conjunto dos números complexos, $\mathbb{C} = \{a + bi, a, b \in \mathbb{R}\}$, onde $i^2 = -1$ e $a + bi = c + di \Leftrightarrow a = c$ e b = d.

Sejam $a, b, c, d \in \mathbb{R}$. As operações + e $\cdot$ em $\mathbb{C}$ são definidas por:

$$\begin{cases} (a+bi) + (c+di) = (a+c) + (b+d)i \\ (a+bi) \cdot (c+di) = (ac - bd) + (ad + bc)i. \end{cases}$$

Não é difícil verificar que $\mathbb{C}$ é um anel comutativo com elemento neutro $0 + 0i$ e elemento unidade $1 + 0i$. Além disso, $\mathbb{C}$ com as operações acima é um corpo. De fato, dado um complexo não-nulo $z = a + bi$, não é difícil ver que $z^{-1} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2}\, i$.

Exemplo 1.4. Seja $\mathbb{R}^4 = \{(a, b, c, d) : a, b, c, d \in \mathbb{R}\}$ onde $(a, b, c, d) = (a_1, b_1, c_1, d_1) \Leftrightarrow a = a_1, b = b_1, c = c_1, d = d_1$.

Sejam $a, b, c, d, a_1, b_1, c_1, d_1 \in \mathbb{R}$. Definimos as operações de soma e produto em $\mathbb{R}^4$ da seguinte forma:

$(a, b, c, d) + (a_1, b_1, c_1, d_1) = (a + a_1, b + b_1, c + c_1, d + d_1)$,
$(a, b, c, d) \cdot (a_1, b_1, c_1, d_1) = (aa_1 - bb_1 - cc_1 - dd_1, ab_1 + ba_1 + cd_1 - c_1d, ac_1 + a_1c + db_1 - d_1b, ad_1 + da_1 + bc_1 - b_1c)$.

Temos que $\mathbb{A} = (\mathbb{R}^4, +, \cdot)$ é um anel cujo elemento neutro é $(0, 0, 0, 0)$. Verificamos que $(1, 0, 0, 0)$ é a unidade deste anel. De fato, seja $(a, b, c, d) \in \mathbb{R}^4$ então $(a, b, c, d) \cdot (1, 0, 0, 0) = (a \cdot 1 - b \cdot 0 - c \cdot 0 - d \cdot 0, a \cdot 0 + b \cdot 1 + c \cdot 0 - 0 \cdot d, a \cdot 0 + 1 \cdot c + d \cdot 0 - 0 \cdot b, a \cdot 0 + d \cdot 1 + b \cdot 0 - 0 \cdot c) = (a, b, c, d)$.

Analogamente, $(1,0,0,0)\cdot(a,b,c,d)=(a,b,c,d)$. Portanto, $(1,0,0,0)$ é o elemento unidade de $\mathbb{A}$.

Este é um exemplo de um anel não-comutativo com unidade. De fato, consideramos os elementos $(0,1,0,0)$ e $(0,0,1,0)$ de $\mathbb{A}$. Não é difícil ver que $(0,1,0,0)\cdot(0,0,1,0)=(0,0,0,1)$ e que $(0,0,1,0)\cdot(0,1,0,0)=(0,0,0,-1)$.

Vamos agora fazer algumas identificações:

$$\begin{aligned} a &\longleftrightarrow (a,0,0,0),\ a\in\mathbb{R}\\ i &\longleftrightarrow (0,1,0,0)\\ j &\longleftrightarrow (0,0,1,0)\\ k &\longleftrightarrow (0,0,0,1)\\ a+bi+cj+dk &\longleftrightarrow (a,b,c,d),\ a,b,c,d\in\mathbb{R}. \end{aligned}$$

A partir destas identificações consideramos o conjunto $\{a+bi+cj+dk : a,b,c,d\in\mathbb{R}\}$, onde $a+bi+cj+dk=a_1+b_1i+c_1j+d_1k \Leftrightarrow a=a_1, b=b_1, c=c_1$ e d = d_1. Este conjunto é denotado por $Quat$.

Não é difícil verificar que $i^2=j^2=k^2=-1$ e que

$$\begin{aligned} &i\cdot j=k, \quad j\cdot k=i \quad \text{e} \quad k\cdot i=j;\\ &j\cdot i=-k, \quad k\cdot j=-i \quad \text{e} \quad i\cdot k=-j. \end{aligned}$$

Sejam $a,b,c,d,a_1,b_1,c_1,d_1\in\mathbb{R}$. Então as operações em Quat são definidas por:

$(a+bi+cj+dk)+(a_1+b_1i+c_1j+d_1k)=(a+a_1)+(b+b_1)i+(c+c_1)j+(d+d_1)k$,
$(a+bi+cj+dk)\cdot(a_1+b_1i+c_1j+d_1k)=(aa_1-bb_1-cc_1-dd_1)+(ab_1+ba_1+cd_1-dc_1)i+(ac_1+ca_1+db_1-bd_1)j+(ad_1+da_1+bc_1-cb_1)k$.

Identificamos assim o anel $(\mathbb{R}^4,+,\cdot)$ com o anel $(Quat,+,\cdot)$, onde $0=0+0i+0j+0k$ e $1=1+0i+0j+0k$ são o elemento neutro e a unidade de $(Quat,+,\cdot)$, respectivamente.

No anel $(Quat,+,\cdot)$ existem infinitas soluções para a equação $x^2=-1$.

De fato, seja $x=a+bi+cj+dk$. Então $x^2=(a^2-b^2-c^2-d^2+2abi+2acj+2adk)=-1$. Logo,

$$\begin{cases} a^2 - b^2 - c^2 - d^2 = -1 \\ 2ab = 0 \\ 2ac = 0 \\ 2ad = 0 \end{cases}$$

Se $a \neq 0$ então $b = c = d = 0$. Logo, $a^2 = -1$ e esta equação não tem solução em $\mathbb{R}$. Assim, $a = 0$ e portanto, $b^2 + c^2 + d^2 = 1$ e esta é a equação de uma esfera em $\mathbb{R}^3$ que é satisfeita por infinitas triplas.

Definição 1.5. *Sejam $(\mathbb{A}, +, \cdot)$ um anel e $\mathbb{B}$ um subconjunto não-vazio de $\mathbb{A}$. Dizemos que $\mathbb{B}$ é um subanel de $\mathbb{A}$ se*
(i) *$\mathbb{B}$ é fechado para as operações do anel $\mathbb{A}$, isto é, para quaisquer $a, b \in \mathbb{B}$*

$$a + b \in \mathbb{B} \quad e \quad ab \in \mathbb{B};$$

(ii) *$\mathbb{B}$ com as operações de $\mathbb{A}$ é um anel.*

A seguir apresentamos um critério para que um subconjunto de um anel seja um subanel.

Proposição 1.6. *Sejam $\mathbb{A}$ um anel e $\mathbb{B}$ um subconjunto de $\mathbb{A}$. Então $\mathbb{B}$ é um subanel de $\mathbb{A}$ se, e somente se, são válidas as seguintes condições:*
(i) $0 \in \mathbb{B}$;
(ii) $x, y \in \mathbb{B}$, $x - y \in \mathbb{B}$;
(iii) $x, y \in \mathbb{B}$, $xy \in \mathbb{B}$.

Demonstração: ($\Rightarrow$) Se $\mathbb{B}$ é um subanel então por definição temos as condições (i), (ii) e (iii).

($\Leftarrow$) Sejam $x, y \in \mathbb{B}$. Como $0 \in \mathbb{B}$ então $0 - y = -y \in \mathbb{B}$. Assim, $x - (-y) = x + y \in \mathbb{B}$. Por (iii), $xy \in \mathbb{B}$. Logo, $\mathbb{B}$ é fechado para as operações do anel $\mathbb{A}$.

Como as propriedades associativa, comutativa e distributiva são hereditárias segue que $\mathbb{B}$ com as operações de $\mathbb{A}$ é um anel e isto termina a demonstração. □

Exemplo 1.7. Considerando as operações usuais: $\mathbb{Z}$ é um subanel de $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{Q}$ é um subanel de $\mathbb{R}$ e $\mathbb{C}$; $\mathbb{R}$ é um subanel de $\mathbb{C}$ e $\mathbb{C}$ é um subanel de $Quat$.

Lembrando que $i^2 = j^2 = k^2 = -1$, temos três cópias de $\mathbb{C}$ em $Quat$, isto é, $\{a+bi+0j+0k, a, b \in \mathbb{R}\}$, $\{a+0i+cj+0k, a, c \in \mathbb{R}\}$ e $\{a+0i+0j+dk, a, d \in \mathbb{R}\}$.

Exemplo 1.8. Considerando o anel $\mathbb{A} = \Im(\mathbb{R})$ do Exemplo 1.2. Seja $\mathbb{B} = \{f \in \mathbb{A} : f(1) = 0\}$. Então $\mathbb{B}$ é subanel de $\mathbb{A}$. De fato, é claro que a função nula pertence a $\mathbb{B}$. Dados $f, g \in \mathbb{B}$, temos que $f - g \in \mathbb{B}$, pois $(f-g)(1) = f(1) - g(1) = 0$ e $fg \in \mathbb{B}$, pois $(fg)(1) = f(1)g(1) = 0$.

Logo, $\mathbb{B}$ é subanel de $\mathbb{A}$.

Exemplo 1.9. Sejam $\mathbb{A}$ um anel e $a \in \mathbb{A}$. Então $\mathbb{B} = \{x \in \mathbb{A} : xa = ax\}$ é subanel de $\mathbb{A}$, chamado centro de $\mathbb{A}$. De fato, é claro que $0 \in \mathbb{B}$. Sejam $x, y \in \mathbb{B}$. Então $x - y \in \mathbb{B}$, pois $(x-y)a = xa - ya = ax - ay = a(x-y)$ e $xy \in \mathbb{B}$, pois $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$.

Logo, $\mathbb{B}$ é subanel de $\mathbb{A}$.

1.2 Ideais

Esta classe de subanéis tem muita relevância no estudo da teoria de anéis em geral. Em nosso trabalho, mais especificamente no capítulo 3, vemos a relação dos ideais com os elementos irredutíves de um domínio de integridade.

Definição 1.10. *Seja $\mathbb{A}$ um anel. Um subconjunto $\mathbb{I}$ de $\mathbb{A}$ é dito um ideal de $\mathbb{A}$ se:*
(i) $0 \in \mathbb{I}$;
(ii) $\forall\ x, y \in \mathbb{I}$, $x + y \in \mathbb{I}$;
(iii) $\forall\ x \in \mathbb{I}$, $-x \in \mathbb{I}$;
(iv) *Dados $a \in \mathbb{A}$ e $x \in \mathbb{I}$, $ax \in \mathbb{I}$ e $xa \in \mathbb{I}$.*

Equivalentemente, podemos substituir (i), (ii), (iii) por
(i)$'$ $\mathbb{I} \neq \emptyset$;
(ii)$'$ $\forall\ x, y \in \mathbb{I}$, $x - y \in \mathbb{I}$;
e a propriedade (iv) permanece.

De fato, se $\mathbb{I} \neq \emptyset$ então existe $z \in \mathbb{I}$. Por (ii)$'$, $z - z = 0 \in \mathbb{I}$. Seja $x \in \mathbb{I}$. Como $0 \in \mathbb{I}$, $0 - x = -x \in \mathbb{I}$, por (ii)$'$ e isto implica (iii). Dados $x, y \in \mathbb{I}$, temos que $-y \in \mathbb{I}$ e portanto, $x - (-y) = x + y \in \mathbb{I}$ e segue (ii).

Temos também que (i), (ii) e (iii) implicam obviamente (i)$'$ e (ii)$'$.

Se $\mathbb{A}$ é um anel comutativo então a propriedade (iv) é escrita como $ax \in \mathbb{A}$, para todo $a \in \mathbb{A}$ e para todo $x \in \mathbb{I}$.

Exemplo 1.11. Seja $\mathbb{A}$ um anel. Então $\{0_A\}$ e o anel $\mathbb{A}$ são ideais de $\mathbb{A}$, chamados ideais triviais de $\mathbb{A}$.

Exemplo 1.12. Dado um inteiro n, os subconjuntos $n\mathbb{Z} = \{0, \pm n, \pm 2n, \cdots\}$ de $\mathbb{Z}$ são ideais de $\mathbb{Z}$. De fato, obviamente $n\mathbb{Z}$ não é vazio. Sejam $x, y \in n\mathbb{Z}$. Então existem $r, s \in \mathbb{Z}$ tais que $x = rn$ e $y = sn$. Logo, $x - y = rn - sn = (r - s)n = n(r - s) \in n\mathbb{Z}$. Sejam $a \in \mathbb{Z}$ e $x \in n\mathbb{Z}$. Então existe $t \in \mathbb{Z}$ tal que $x = nt$. Assim, $xa = ax = a(nt) = (an)t = (na)t = n(at) \in n\mathbb{Z}$.

Agora um exemplo de ideais no anel $\mathbb{A} = \Im[0, 1]$ das funções contínuas de $[0, 1]$ em $\mathbb{R}$ com as operações $+$ e $\cdot$ definidas no Exemplo 1.2.

Exemplo 1.13. Seja $b \in [0, 1]$ fixo. Consideramos $\mathbb{I} = \{f \in \mathbb{A} : f(b) = 0\}$. Afirmamos que $\mathbb{I}$ é um ideal de $\mathbb{A}$. De fato, $\mathbb{I} \neq \emptyset$, pois a função nula pertence a $\mathbb{I}$. Sejam $h \in \mathbb{A}$ e $f, g \in \mathbb{I}$. Então $(f - g)(b) = f(b) - g(b) = 0$ e portanto, $f - g \in \mathbb{I}$. Além disso, $(hf)(b) = (fh)(b) = f(b)h(b) = 0$ e daí, $fh = hf \in \mathbb{I}$. Donde segue que $\mathbb{I}$ é um ideal de $\mathbb{A}$.

Quando trabalhamos com anéis não-comutativos podemos estender a noção de ideal, definindo ideais à esquerda e à direita.

Sejam $\mathbb{A}$ um anel e $\mathbb{I}$ um subanel de $\mathbb{A}$. Dizemos que $\mathbb{I}$ é um ideal à esquerda de $\mathbb{A}$ se para quaisquer $a \in \mathbb{A}$ e $x \in \mathbb{I}$, $ax \in \mathbb{I}$ (ou $\mathbb{A}\mathbb{I} \subseteq \mathbb{I}$). Analogamente, se para quaisquer $a \in \mathbb{A}$ e $x \in \mathbb{I}$, $xa \in \mathbb{I}$ (ou $\mathbb{I}\mathbb{A} \subseteq \mathbb{I}$) dizemos que $\mathbb{I}$ é um ideal à direita de $\mathbb{A}$. Se $\mathbb{I}$ é um ideal à direita e à esquerda de $\mathbb{A}$, então $\mathbb{I}$ é dito um ideal de $\mathbb{A}$.

Notamos que se $\mathbb{I}$ é ideal então $\mathbb{I}$ é ideal à esquerda e à direita. No entanto, $\mathbb{I}$ pode ser ideal à esquerda ou à direita e não ser um ideal, como mostramos abaixo.

Exemplo 1.14. Seja $\mathbb{A} = \mathbb{M}_2(\mathbb{R})$, o anel das matrizes de ordem 2 com entradas reais. Sejam $\mathbb{I}$ e $\mathbb{J}$ definidos como segue

$$\mathbb{I} = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\} \quad \text{e} \quad \mathbb{J} = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

Então $\mathbb{I}$ é um ideal à esquerda de $\mathbb{A}$ e $\mathbb{J}$ é um ideal à direita de $\mathbb{A}$ mas nenhum dos dois é um ideal de $\mathbb{A}$.

É fácil ver que $\mathbb{I}$ e $\mathbb{J}$ são subanéis de $\mathbb{A}$. Mostramos então que $\mathbb{I}$ e $\mathbb{J}$ são, respectivamente, ideais à esquerda e à direita de $\mathbb{A}$. De fato, sejam

$A = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathbb{A}$ e $B = \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in \mathbb{I}$. Então

$AB = \begin{pmatrix} xa+yb & 0 \\ za+wb & 0 \end{pmatrix} \in \mathbb{I}$. Logo, $\mathbb{I}$ é um ideal à esquerda de $\mathbb{A}$.

Mas, por exemplo, tomando os elementos

$A = \begin{pmatrix} 1 & -2 \\ -1 & 0 \end{pmatrix} \in \mathbb{A}$ e $B = \begin{pmatrix} 2 & 0 \\ 3 & 0 \end{pmatrix} \in \mathbb{I}$, vemos que $BA \notin \mathbb{I}$. Portanto, $\mathbb{I}$ não é um ideal à direita de $\mathbb{A}$ e obviamente não é um ideal de $\mathbb{A}$.

Agora verificamos que $\mathbb{J}$ é um ideal à direita de $\mathbb{A}$, mas não é um ideal de $\mathbb{A}$. De fato, sejam

$A = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathbb{A}$ e $C = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in \mathbb{J}$. Então

$CA = \begin{pmatrix} ax+bz & ay+bw \\ 0 & 0 \end{pmatrix} \in \mathbb{J}$ e portanto $\mathbb{J}$ é um ideal à direita de $\mathbb{A}$.

Tomando os elementos

$A = \begin{pmatrix} 2 & 3 \\ -1 & 6 \end{pmatrix} \in \mathbb{A}$ e $C = \begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix} \in \mathbb{J}$, vemos que $AC \notin \mathbb{J}$. Portanto, $\mathbb{J}$ não é um ideal à esquerda de $\mathbb{A}$ e obviamente não é um ideal de $\mathbb{A}$.

Estudamos abaixo ideais que são finitamente gerados, ideais obtidos de uma interseção arbitrária de outros ideais de um anel e ideais obtidos de uma união de ideais encaixados de um anel.

Proposição 1.15. *Sejam $\mathbb{A}$ um anel comutativo e $x_1, x_2, \cdots, x_n \in \mathbb{A}$. Consideramos o conjunto $\mathbb{I} = Ax_1 + Ax_2 + \cdots + Ax_n = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : a_i \in \mathbb{A}\}$. Então $\mathbb{I}$ é um ideal de $\mathbb{A}$.*

Demonstração: $\mathbb{I}$ é claramente não-vazio. Sejam $x, y \in \mathbb{I}$. Então, temos que $x = a_1x_1 + \cdots + a_nx_n$ e $y = b_1x_1 + \cdots + b_nx_n$.

Logo, $x - y = (a_1 - b_1)x_1 + \cdots + (a_n - b_n)x_n \in \mathbb{I}$. Para todo $c \in \mathbb{A}$ temos que $xc = cx = ca_1x_1 + \cdots + ca_nx_n \in \mathbb{I}$. Portanto, $\mathbb{I}$ é um ideal de $\mathbb{A}$. □

Esse ideal é dito o ideal gerado por $x_1, x_2, \cdots, x_n$ e denotamos por $\mathbb{I} = (x_1, x_2, \cdots, x_n)$. No caso em que $\mathbb{I} = (x) = \{ax : a \in \mathbb{A}\}$, isto é, $\mathbb{I}$ é gerado por apenas um elemento $x \in \mathbb{A}$, $\mathbb{I}$ é dito um ideal principal de $\mathbb{A}$.

Por exemplo, $2\mathbb{Z}$ é um ideal principal de $\mathbb{Z}$ gerado pelo elemento 2. Na verdade, $\mathbb{Z}$ é um domínio de ideais principais, isto é, todo ideal de $\mathbb{Z}$ é principal. Este fato é mostrado no Capítulo 3.

Se $\mathbb{A}$ é um anel não comutativo então o conjunto $\mathbb{I}$ definido acima é apenas um ideal à esquerda de $\mathbb{A}$.

Proposição 1.16. *Seja $\mathbb{A}$ um anel qualquer. Sejam $\mathbb{I}$ e $\mathbb{J}$ ideais de $\mathbb{A}$. Então $\mathbb{I} \cap \mathbb{J}$ é um ideal de $\mathbb{A}$.*

Demonstração: Claramente, $\mathbb{I} \cap \mathbb{J}$ é não-vazio, pois $0 \in \mathbb{I} \cap \mathbb{J}$. Sejam $x, y \in \mathbb{I} \cap \mathbb{J}$. Então $x, y \in \mathbb{I}$ e $x, y \in \mathbb{J}$. Logo, $x - y \in \mathbb{I}$ e $x - y \in \mathbb{J}$ e daí, $x - y \in \mathbb{I} \cap \mathbb{J}$.

Sejam $x \in \mathbb{I} \cap \mathbb{J}$ e $a \in \mathbb{A}$. Como $\mathbb{I}$ e $\mathbb{J}$ são ideais, temos que $ax \in \mathbb{I}$ e $ax \in \mathbb{J}$ e também que $xa \in \mathbb{I}$ e $xa \in \mathbb{J}$. Logo, $ax \in \mathbb{I} \cap \mathbb{J}$ e $xa \in \mathbb{I} \cap \mathbb{J}$. □

A proposição acima pode ser estendida para uma família qualquer de ideais de um anel $\mathbb{A}$.

Proposição 1.17. *Sejam $\mathbb{A}$ um anel e $\{I_i\}_{i \in \Omega}$ uma família de ideais de $\mathbb{A}$, onde Ω é um conjunto de índices qualquer. Então $\bigcap_{i \in \Omega} I_i$ é um ideal de $\mathbb{A}$.*

Proposição 1.18. *Sejam $\mathbb{A}$ um anel e $\{I_n\}_{n \in \mathbb{N}}$ uma família de ideais de um anel $\mathbb{A}$. Se $I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \cdots \subseteq \cdots$ então $\mathbb{I} = \bigcup_{i \in \mathbb{N}} I_i$ é um ideal de $\mathbb{A}$.*

Demonstração: Claramente $\mathbb{I}$ é não-vazio, pois $0 \in I_0$ por exemplo. Sejam x e y elementos de $\mathbb{I}$. Então existem $r, s \in \mathbb{N}$ tais que $x \in I_r$ e $y \in I_s$. Podemos supor, sem perda de generalidade, que $r \leq s$. Assim $x \in I_s$, pois $x \in I_r \subseteq I_s$. Sendo I_s um ideal segue que $x - y \in I_s$. Logo, $x - y \in \mathbb{I}$.

Sejam $x \in \mathbb{I}$ e $y \in \mathbb{A}$. Então $x \in I_j$, para algum $j \in \mathbb{N}$. Sendo I_j um ideal de $\mathbb{A}$ segue que $xy \in I_j$ e $yx \in I_j$. Donde, $xy \in \mathbb{I}$ e $yx \in \mathbb{I}$. □

Observação: É importante notarmos que na proposição acima a hipótese $\mathbb{I}_i \subseteq \mathbb{I}_{i+1}$, $i \in \mathbb{N}$, é essencial. De fato, sejam $\mathbb{A} = \mathbb{Z}$, $\mathbb{I}_0 = 3\mathbb{Z}$ e $\mathbb{I}_1 = 5\mathbb{Z}$. Então

$\mathbb{I}_0 \cup \mathbb{I}_1$ não é um ideal de $\mathbb{Z}$, pois $3 + 5 = 8$ não pertence a união de $\mathbb{I}_0$ e I_1. Assim, obtém-se que a união arbitrária de ideais nem sempre é um ideal.

Definição 1.19. *Seja $\mathbb{M}$ um ideal de um anel comutativo $\mathbb{A}$. $\mathbb{M}$ é dito um ideal maximal se*
(i) $\mathbb{M} \neq \mathbb{A}$*;*
(ii) *Se $\mathbb{I}$ é um ideal de $\mathbb{A}$ tal que $\mathbb{M} \subseteq \mathbb{I} \subseteq \mathbb{A}$, então $\mathbb{I} = \mathbb{M}$ ou $\mathbb{I} = \mathbb{A}$.*

Para provar o teorema abaixo, usamos o fato de que todo ideal de $\mathbb{Z}$ é principal, embora este seja provado apenas no Capítulo 3.

Teorema 1.20. *Seja $p \in \mathbb{Z}$. Então $p\mathbb{Z}$ é um ideal maximal de $\mathbb{Z}$ se, e somente se, p é um número primo, isto é, os únicos divisores de p em $\mathbb{Z}$ são ± 1 e $\pm p$.*

Demonstração: Suponhamos que p seja um número primo. Claramente, $p\mathbb{Z} \neq \mathbb{Z}$. Seja $\mathbb{I}$ um ideal de $\mathbb{Z}$ tal que $p\mathbb{Z} \subseteq \mathbb{I} \subseteq \mathbb{Z}$. Temos que $\mathbb{I} = (n)$, pois $\mathbb{Z}$ é principal e como $p \in \mathbb{I}$, segue que $p = nq$, para algum $q \in \mathbb{Z}$. Portanto n divide p e sendo p primo, vem que $n = \pm 1$ ou $n = \pm p$. Assim, $\mathbb{I} = \mathbb{Z}$ ou $\mathbb{I} = p\mathbb{Z}$. Logo, $p\mathbb{Z}$ é um ideal maximal.

Reciprocamente, temos que $p\mathbb{Z} \neq \mathbb{Z}$ e portanto, $p \neq \pm 1$. Suponhamos $n \in \mathbb{Z}$ tal que n divide p. Logo, $p \in (n)$. Sendo $p\mathbb{Z}$ maximal, segue que $(n) = p\mathbb{Z}$ ou $(n) = \mathbb{Z}$. Logo, $n = \pm p$ ou $n = \pm 1$. □

Exemplo 1.21. São exemplos de ideais maximais em $\mathbb{Z}$: $2\mathbb{Z}, 3\mathbb{Z}, 11\mathbb{Z}$, etc.

Capítulo 2

Domínios de Integridade

Neste capítulo apresentamos definições e propriedades importantes de um domínio de integridade.

Na última seção desse capítulo estudamos os anéis quadráticos, que são exemplos importantes de domínios de integridade. Estes anéis são interessantes, pois neles conseguimos exemplos onde nem sempre existe máximo divisor comum de dois de seus elementos, exemplos de elementos irredutíveis que não são primos, etc.

Em todo este capítulo, $\mathbb{A}$ é um domínio de integridade.

2.1 Divisibilidade em um Domínio de Integridade

Definição 2.1. *Sejam a e b elementos de $\mathbb{A}$. Dizemos que a divide b se existe c em $\mathbb{A}$ tal que $b = ac$.*

Usamos a notação $a|b$ para indicar que a divide b ou b é divisível por a.

Proposição 2.2. *A relação de divisibilidade definida acima goza das seguintes propriedades:*

(i) *Reflexiva:* De fato, como $\mathbb{A}$ possui elemento unidade 1, basta notar que $a = a\,1$, isto é, $a|a$.

(ii) *Transitiva:* Suponhamos que $a|b$ e $b|c$. Então existem d e $d^{'}$ em $\mathbb{A}$ tais

que $b = ad$ e $c = bd'$. Logo, $c = a(dd')$, isto é, $a|c$.

(iii) *Se $a|b$ e $a|c$ então $a|(bx + cy)$ para quaisquer $x, y \in \mathbb{A}$.* De fato, existem d e d' em $\mathbb{A}$ tais que $b = ad$ e $c = ad'$. Para quaisquer $x, y \in \mathbb{A}$ temos que $bx = adx$ e $cy = ad'y$. Portanto, $bx + cy = a(dx + d'y)$, ou seja, $a|(bx + cy)$.

Em particular, se $a|b$ e $a|c$ então $a|(b \pm c)$ e $a|bx$ para todo $x \in \mathbb{A}$.

(iv) *Se $a|b$, então $ac|bc$.* De fato, existe $d \in \mathbb{A}$ tal que $b = ad$. Assim, $bc = adc = (ac)d$. Logo, $ac|bc$.

Corolário 2.3. *Sejam a, b e $c \in \mathbb{A}$, com $c \neq 0$. Então $a|b$ se, e somente se, $ac|bc$.*

Definição 2.4. *Sejam a e b elementos de $\mathbb{A}$. Dizemos que a é associado de b se, e somente se, $a|b$ e $b|a$.*

Usamos a notação $a \sim b$ para indicar que a é associado de b.

A relação $\sim$ definida acima é uma relação de equivalência. De fato, sejam $a, b, c \in \mathbb{A}$. É claro que $\sim$ é reflexiva, pois $a|a$. A propriedade simétrica é facilmente verificada. Suponhamos que $a \sim b$ e que $b \sim c$. Então $a|b$ e $b|a$ e $b|c$ e $c|b$. Como a divisibilidade é transitiva, veja a propriedade (ii) anterior, segue que $a|c$ e $c|a$, isto é, $a \sim c$.

Definição 2.5. *Um elemento $a \in \mathbb{A}$ é dito invertível em $\mathbb{A}$ se existe $b \in \mathbb{A}$ tal que $ab = ba = 1$.*

O conjunto de todos os elementos invertíveis de $\mathbb{A}$ é denotado por $\mathbb{U}(\mathbb{A})$.

Exemplo 2.6. Dois elementos não-nulos quaisquer de um corpo qualquer $\mathbb{K}$ são associados.

De fato, sejam a e b elementos não-nulos de $\mathbb{K}$. Como $\mathbb{U}(\mathbb{K}) = \mathbb{K}^*$, temos que existe $b^{-1} \in \mathbb{K}$ tal que $bb^{-1} = 1$. Assim, $a = b(b^{-1}a)$ e portanto, $b|a$. Analogamente $a|b$. Logo, a e b são associados em $\mathbb{K}$.

Exemplo 2.7. Dois números inteiros a e b são associados se, e somente se, $a = b$ ou $a = -b$.

De fato, no anel $\mathbb{Z}$, os únicos elementos invertíveis são ± 1. Sejam $a, b \in \mathbb{Z}$ tais que $a|b$ e $b|a$. Então existem $c, c' \in \mathbb{Z}$ tais que $b = ac$ e $a = bc'$. Logo, $b = bc'c$ o que implica $c'c = 1$. Logo, $c = c' = \pm 1$. Assim, $a = b$ ou $a = -b$. A afirmação contrária é óbvia.

Proposição 2.8. *Sejam a e b elementos quaisquer de $\mathbb{A}$. Então são equivalentes as seguintes afirmações:*

(i) $a \sim b$;

(ii) $(a) = (b)$;

(iii) *Existe um elemento invertível $u \in \mathbb{A}$ tal que $b = au$.*

Demonstração: (i) $\Rightarrow$ (ii) Como $a \sim b$ então $a|b$ e $b|a$, ou seja, existem d e $d^{'}$ em $\mathbb{A}$ tais que $b = ad$ e $a = bd^{'}$. Seja $x \in (a)$. Então existe $c \in \mathbb{A}$ tal que $x = ac$. Assim, $x = b(d^{'}c)$ e portanto $x \in (b)$. Logo, $(a) \subseteq (b)$. Analogamente mostramos que $(b) \subseteq (a)$.

(ii) $\Rightarrow$ (iii) Temos que $b \in (a)$, então existe $d_1 \in \mathbb{A}$ tal que $b = ad_1$. Também $a \in (b)$ e portanto, $a = bd_2$, para algum $d_2 \in \mathbb{A}$. Assim, $a = bd_2 = ad_1d_2$ e isto implica que $a(1 - d_1d_2) = 0$.

Se $a = 0$ então é claro que $b = 0$ e $b = 1a$.

Se $d_1d_2 = 1$ então d_1 e d_2 são elementos invertíveis em $\mathbb{A}$ e como $b = ad_1$ segue (iii).

(iii) $\Rightarrow$ (i) Sendo que $b = au$ para algum elemento invertível $u \in \mathbb{A}$, segue que $a|b$. Temos que existe $u^{'} \in \mathbb{A}$ tal que $uu^{'} = 1$. Assim $bu^{'} = auu^{'} = a$, isto é, $b|a$. Portanto, $a \sim b$. □

Definição 2.9. *Dizemos que um elemento $p \in \mathbb{A}$ é primo se, e somente se, $p \neq 0$, p não é invertível em $\mathbb{A}$ e se $p|ab$ então $p|a$ ou $p|b$, para $a, b \in \mathbb{A}$.*

Proposição 2.10. *Se p é primo e $p|a_1a_2 \cdots a_n$ com $a_i \in \mathbb{A}$ e $n \geq 1$, então p divide pelo menos um dos fatores a_i.*

Demonstração: Usamos indução finita. Para $n = 1$ segue diretamente que $p|a_1$.

Suponhamos por hipótese de indução que para $n = k$, $p|a_i$ para algum $i \in \{1, 2, \cdots, k\}$.

Agora admitimos que $p|a_1a_2 \cdots a_ka_{k+1}$. Pela definição de elemento primo, temos que $p|a_1a_2 \cdots a_k$ ou $p|a_{k+1}$. Se $p|a_{k+1}$ o resultado segue. Se $p|a_1a_2 \cdots a_k$ então pela hipótese de indução $p|a_i$ para algum $1 \leq i \leq k$ e fica provado o resultado. □

Definição 2.11. *Dizemos que um elemento $p \in \mathbb{A}$ é irredutível se, e somente se, $p \neq 0$, $p \notin \mathbb{U}(\mathbb{A})$ e se $p = ab$ para $a, b \in \mathbb{A}$ então $a \in \mathbb{U}(\mathbb{A})$ ou $b \in \mathbb{U}(\mathbb{A})$.*

Proposição 2.12. *Todo elemento primo em $\mathbb{A}$ é irredutível.*

Demonstração: Seja $p \in \mathbb{A}$ um elemento primo. Então $p \neq 0$ e p não é invertível.

Sejam $a, b \in \mathbb{A}$ tais que $p = ab$. Então $p|a$ ou $p|b$, pois p é primo. Suponhamos que $p|a$, então existe $c \in \mathbb{A}$ tal que $a = pc$. Logo, $p = pcb$ e isto implica que $cb = 1$, pois $p \neq 0$. Logo, b é invertível em $\mathbb{A}$. Analogamente, se $p|b$ então a é invertível em $\mathbb{A}$. □

2.2 Máximo Divisor Comum

Definição 2.13. *Dizemos que um elemento $d \in \mathbb{A}$ é máximo divisor comum dos elementos $a, b \in \mathbb{A}$ se*
(i) *$d|a$ e $d|b$;*
(ii) *Se $d_1 \in \mathbb{A}$ é tal que $d_1|a$ e $d_1|b$ então $d_1|d$.*

Usamos a notação $mdc(a, b) = d$ para indicar que d é um máximo divisor comum de a e b.

Proposição 2.14. *Se $d = mdc(a, b)$ então um elemento $d_1 \in \mathbb{A}$ também é um máximo divisor comum de a e b se, e somente se, $d_1 \sim d$.*

Demonstração: ($\Rightarrow$) De fato, temos que $d = mdc(a, b)$ e por hipótese d_1 é um máximo divisor comum de a e b. Pela definição, é imediato que $d_1|d$ e $d|d_1$. Logo $d_1 \sim d$.

($\Leftarrow$) Seja $d_1 \in \mathbb{A}$ um associado de d. Então $d_1|d$ e $d|d_1$ e sendo $d = mdc(a, b)$, segue que $d|a$ e $d|b$. Logo $d_1|a$ e $d_1|b$, devido à transitividade da divisibilidade. Suponhamos que exista $d_2 \in \mathbb{A}$ tal que $d_2|a$ e $d_2|b$. Pela definição de máximo divisor comum, $d_2|d$ e como $d|d_1$, vem que $d_2|d_1$. Logo, d_1 é um máximo divisor comum de a e b. □

Observamos então que o máximo divisor comum de dois elementos de $\mathbb{A}$, caso exista, não é em geral determinado de modo único. No caso do anel dos inteiros por exemplo, pedimos que o máximo divisor comum seja positivo.

Sejam $a, b \in \mathbb{A}$. Dizemos que a e b são primos entre si se a unidade de $\mathbb{A}$ é um máximo divisor comum desses elementos.

2.3 Anéis Quadráticos

Os anéis quadráticos desempenham um papel importante em nosso trabalho, pois são domínios de integridade onde encontramos exemplos interessantes.

Seja $n \neq 1$ um número inteiro livre de quadrados, ou seja, n não é divisível por nenhum quadrado perfeito, salvo o número 1.

Indicamos por $\mathbb{Z}[\sqrt{n}\,]$ o seguinte subconjunto de $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{n}\,] = \{a + b\sqrt{n} : a, b \in \mathbb{Z}\}.$$

Para cada n nas condições acima, $\mathbb{Z}[\sqrt{n}\,]$ é um subanel de $\mathbb{C}$, onde para cada $\alpha = a + b\sqrt{n}$ e $\beta = c + d\sqrt{n}$ com $a, b, c, d \in \mathbb{Z}$, temos que

$$\begin{aligned} \alpha + \beta &= (a + b\sqrt{n}) + (c + d\sqrt{n}) = (a + c) + (b + d)\sqrt{n}\,; \\ \alpha\beta &= (a + b\sqrt{n})(c + d\sqrt{n}) = (ac + bdn) + (ad + bc)\sqrt{n}. \end{aligned}$$

Obviamente, $\mathbb{Z}[\sqrt{n}\,]$ é um anel com essas operações e é um domíno de integridade, pois é um subanel de $\mathbb{C}$. Para cada n, $\mathbb{Z}[\sqrt{n}\,]$ é chamado *anel quadrático.*

No caso em que $n = -1$, o anel $\mathbb{Z}[\sqrt{-1}\,]$ é chamado *anel dos inteiros de Gauss.*

Além disso, $\alpha = a + b\sqrt{n}$ e $\beta = c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}\,]$ são iguais se, e somente se, $a = c$ e $b = d$.

Seja $\alpha = a + b\sqrt{n} \in \mathbb{Z}[\sqrt{n}\,]$. A norma de α, indicada por $N(\alpha)$, é definida do seguinte modo:

$$N(\alpha) = a^2 - b^2 n.$$

Obviamente, $N(\alpha) \in \mathbb{Z}$.

Proposição 2.15. *Sejam $\alpha = a + b\sqrt{n}$, $\beta = c + d\sqrt{n} \in \mathbb{Z}[\sqrt{n}\,]$. Então valem as seguintes propriedades:*

(i) $N(\alpha) = 0$ *se, e somente se,* $\alpha = 0$.

(ii) $N(\alpha\beta) = N(\alpha)N(\beta)$.

(iii) $N(1) = 1$.

(iv) $N(\alpha) = \pm 1$ *se, e somente se,* α *é invertível em* $\mathbb{Z}[\sqrt{n}\,]$.

(v) *Se* $N(\alpha)$ *é um número primo então* α *é irredutível em* $\mathbb{Z}[\sqrt{n}\,]$.

Demonstração: (i) $N(\alpha) = 0 \Leftrightarrow a^2 - b^2 n = 0 \Leftrightarrow a^2 = b^2 n \Leftrightarrow a = b = 0 \Leftrightarrow \alpha = 0$.

(ii) Temos que $\alpha\beta = (ac + bdn) + (ad + bc)\sqrt{n}$. Logo,

$$\begin{aligned} N(\alpha\beta) &= (ac + bdn)^2 - (ad + bc)^2 n = a^2(c^2 - d^2 n) - b^2 n(c^2 - d^2 n) \\ &= (a^2 - b^2 n)(c^2 - d^2 n) = N(\alpha)N(\beta). \end{aligned}$$

(iii) É óbvio.

(iv) ($\Rightarrow$) Suponhamos $N(\alpha) = a^2 - b^2 n = 1$. Como $(a + b\sqrt{n})(a - b\sqrt{n}) = N(\alpha)$, segue que $\alpha|1$. Logo, α é invertível em $\mathbb{Z}[\sqrt{n}\,]$. O mesmo se $N(\alpha) = -1$.

($\Leftarrow$) Suponhamos α invertível em $\mathbb{Z}[\sqrt{n}\,]$. Então existe $\beta \in \mathbb{Z}[\sqrt{n}\,]$ tal que $\alpha\beta = 1$ e isto implica que $N(\alpha)N(\beta) = N(\alpha\beta) = 1$. Logo, $N(\alpha)|1$ (em $\mathbb{Z}$) e portanto, $N(\alpha) = \pm 1$.

(v) Sendo $N(\alpha) = p$, onde p é um número primo, então $\alpha \neq 0$ e α não é invertível. Suponhamos que $\alpha = \beta\gamma$, onde β e $\gamma \in \mathbb{Z}[\sqrt{n}\,]$. Então $p = N(\beta)N(\gamma)$. Logo, $N(\beta) = \pm 1$ ou $N(\gamma) = \pm 1$ e isto nos diz que β é invertível ou γ é invertível. Portanto, α é irredutível em $\mathbb{Z}[\sqrt{n}\,]$. □

Exemplo 2.16. Considerando $\mathbb{Z}[\sqrt{-1}\,]$ o anel dos inteiros de Gauss, temos que $\mathbb{U}(\mathbb{Z}[\sqrt{-1}\,]) = \{\pm 1, \pm\sqrt{-1}\}$.

De fato, seja $\alpha = a + b\sqrt{-1}$ um elemento invertível em $\mathbb{Z}[\sqrt{-1}\,]$. Pela propriedade (iv) da Proposição 2.15, $N(\alpha) = a^2 + b^2 = 1$. Em $\mathbb{Z}$, podem ocorrer as possibilidades:

(i) $a^2 = 1$ e $b = 0$ e isto implica que $\alpha = \pm 1$;

(ii) $a = 0$ e $b^2 = 1$, ou seja, $\alpha = \pm\sqrt{-1}$.

Portanto, $\mathbb{U}(\mathbb{Z}[\sqrt{-1}\,]) = \{\pm 1, \pm\sqrt{-1}\}$.

A recíproca da Proposição 2.12 é falsa, vemos um exemplo disso abaixo.

Exemplo 2.17. Seja o anel quadrático $\mathbb{Z}[\sqrt{-11}\,]$. Vamos mostrar que $\mathbb{U}(\mathbb{Z}[\sqrt{-11}\,]) = \{\pm 1\}$ e que 3 é irredutível neste anel, mas não é primo.

Seja $\alpha = a + b\sqrt{-11} \in \mathbb{Z}[\sqrt{-11}\,]$ um elemento invertível. Pela propriedade (iv) da norma, temos que $N(\alpha) = a^2 + 11b^2 = 1$. Como a e b são inteiros temos $a = \pm 1$ e $b = 0$. Logo, os únicos elementos invertíveis de $\mathbb{Z}[\sqrt{-11}\,]$ são $\{\pm 1\}$.

Verificamos agora que 3 é irredutível.

Suponhamos $3 = (a + b\sqrt{-11})(c + d\sqrt{-11}), a, b, c, d \in \mathbb{Z}$. Aplicando a norma temos que $9 = (a^2 + 11b^2)(c^2 + 11d^2)$. Em $\mathbb{Z}$ temos apenas as possibilidades:

(i) $a^2 + 11b^2 = 3$ e $c^2 + 11d^2 = 3$;

(ii) $a^2 + 11b^2 = 1$ e $c^2 + 11d^2 = 9$.

A possibilidade (i) é claramente impossível em $\mathbb{Z}$. A segunda possibilidade é possível e, neste caso, $a^2 + 11b^2 = 1$ e $c^2 + 11d^2 = 9$ ou vice-versa.

Se $a^2 + 11b^2 = 1$ então $a + b\sqrt{-11}$ é invertível e se $a^2 + 11b^2 = 9$ então $c^2 + 11d^2 = 1$ e assim, $c + d\sqrt{-11}$ é invertível. Donde 3 é irredutível em $\mathbb{A}$.

Verificamos que 3 não é primo em $\mathbb{Z}[\sqrt{-11}\,]$.

Temos que $3|(2 + \sqrt{-11})(2 - \sqrt{-11})$, pois $(2 + \sqrt{-11})(2 - \sqrt{-11}) = 15$, mas 3 não divide $(2 + \sqrt{-11})$ e 3 não divide $2 - \sqrt{-11}$. De fato, supondo que 3 divida $2 + \sqrt{-11}$ então $2 + \sqrt{-11} = 3(a + b\sqrt{-11})$ para alguns $a, b \in \mathbb{Z}$ e isto implica que $3a = 2$ e $3b = 1$, o que é um absurdo. Analogamente, mostramos que 3 não divide $2 - \sqrt{-11}$ em $\mathbb{Z}[\sqrt{-11}\,]$. Logo, 3 não é primo em $\mathbb{Z}[\sqrt{-11}\,]$.

Apresentamos agora um exemplo onde calculamos um máximo divisor comum e outro onde mostramos que nem sempre é possível obter máximo divisor comum num anel quadrático.

Exemplo 2.18. O número 1 é um máximo divisor comum de 2 e $1 + 2\sqrt{-1}$ em $\mathbb{Z}[\sqrt{-1}\,]$.

De fato, como $N(1 + 2\sqrt{-1}) = 5$, segue de (v) da Proposição 2.15 que $1 + 2\sqrt{-1}$ é irredutível em $\mathbb{Z}[\sqrt{-1}\,]$. Logo, se $1 + 2\sqrt{-1} = (a + b\sqrt{-1})(c + d\sqrt{-1})$ então $a + b\sqrt{-1} \in \mathbb{U}(\mathbb{Z}[\sqrt{-1}\,])$ ou $c + d\sqrt{-1} \in \mathbb{U}(\mathbb{Z}[\sqrt{-1}\,])$.

Sabemos do Exemplo 2.16 que $\mathbb{U}(\mathbb{Z}[\sqrt{-1}\,]) = \{\pm 1, \pm\sqrt{-1}\}$. Portanto, quando $a + b\sqrt{-1} = \pm 1$ teremos que $c + d\sqrt{-1} = \pm(1 + 2\sqrt{-1})$. No outro caso, isto é, se $a + b\sqrt{-1} = \pm\sqrt{-1}$ então $c + d\sqrt{-1} = \pm 2 \mp \sqrt{-1}$.

Logo, $\{\pm 1, \pm\sqrt{-1}, \pm(1+2\sqrt{-1}), \pm 2 \mp \sqrt{-1}\}$ são os divisores de $1+2\sqrt{-1}$ em $\mathbb{Z}[\sqrt{-1}\,]$.

Não é difícil ver que $\{\pm 1, \pm\sqrt{-1}, \pm 2, \pm 2\sqrt{-1}, \pm(1+\sqrt{-1}), \pm 1 \mp \sqrt{-1}\}$ são os divisores de 2 em $\mathbb{Z}[\sqrt{-1}\,]$, pois se $2 = \alpha\beta$, onde $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}\,]$ então $N(\alpha)N(\beta) = 4$, podendo ocorrer $N(\alpha) = 1$ e $N(\beta) = 4$ (e vice-versa) e $N(\alpha) = 2$ e $N(\beta) = 2$.

Logo, o conjunto dos divisores comuns de 2 e $1+2\sqrt{-1}$ em $\mathbb{Z}[\sqrt{-1}\,]$ é exatamente $\mathbb{U}(\mathbb{Z}[\sqrt{-1}\,])$. Claramente 1 satisfaz a condição (ii) da definição de máximo divisor comum. Portanto, 1 é um $mdc(2, 1+2\sqrt{-1})$ indicando que eles são relativamente primos entre si.

Exemplo 2.19. Consideramos o anel quadrático $\mathbb{Z}[\sqrt{-5}\,]$, os elementos 9 e $6+3\sqrt{-5}$ não admitem máximo divisor comum neste anel.

Primeiramente achamos os divisores de 9 em $\mathbb{Z}[\sqrt{-5}\,]$. Suponhamos que $9 = \alpha\beta$, com $\alpha = a + b\sqrt{-5}$ e $\beta = c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}\,]$. Então, $81 = N(\alpha)N(\beta)$. Temos as seguintes possibilidades:

(i) $N(\alpha) = 1$ e $N(\beta) = 81$ (e vice-versa).

Temos $N(\alpha) = a^2 + 5b^2 = 1$ e $N(\beta) = c^2 + 5d^2 = 81$. Neste caso, $\alpha = \pm 1$ e $\beta = \pm 1 \pm 4\sqrt{-5}$ ou $\beta = \pm 6 \pm 3\sqrt{-5}$ ou $\beta = \pm 9$. Como $\alpha\beta = 9$ segue que $\alpha = 1$ e $\beta = 9$ ou $\alpha = -1$ e $\beta = -9$.

(ii) $N(\alpha) = 3$ e $N(\beta) = 27$ (e vice-versa).

A equação $N(\alpha) = a^2 + 5b^2 = 3$ claramente não possui soluções inteiras. Logo, esta possibilidade não ocorre.

(iii) $N(\alpha) = 9$ e $N(\beta) = 9$.

Temos que $N(\alpha) = a^2 + 5b^2 = 9$ e $N(\beta) = c^2 + 5d^2 = 9$. Então $\alpha = \pm 3$ ou $\alpha = \pm 2 \pm \sqrt{-5}$. O mesmo para β. Como $\alpha\beta = 9$ segue que $\alpha = \beta = 3$ ou $\alpha = \beta = -3$ ou $\alpha = 2 + \sqrt{-5}$ e $\beta = 2 - \sqrt{-5}$ ou $\alpha = -2 - \sqrt{-5}$ e $\beta = -2 + \sqrt{-5}$.

De (i), (ii) e (iii) concluímos que os divisores de 9 em $\mathbb{Z}[\sqrt{-5}\,]$ são $\{\pm 1, \pm 3, \pm 9, \pm 2 \pm \sqrt{-5}\}$.

Agora observando que $N(6 + 3\sqrt{-5}) = 81$ e usando o mesmo raciocínio acima obtemos que $\{\pm 1, \pm 3, \pm(6 + 3\sqrt{-5}), \pm(2 + \sqrt{-5})\}$ são os divisores de $6 + 3\sqrt{-5}$ em $\mathbb{Z}[\sqrt{-5}\,]$.

Logo, $\{\pm 1, \pm 3, 2 + \sqrt{-5}, -2 - \sqrt{-5}\}$ são os divisores comuns de 9 e $6 + 3\sqrt{-5}$ em $\mathbb{Z}[\sqrt{-5}\,]$.

A condição (ii) da definição de máximo divisor comum falha para os divisores comuns acima. De fato, é claro que 3 não divide ± 1, $2 + \sqrt{-5}$ e $-2 - \sqrt{-5}$ em $\mathbb{Z}[\sqrt{-5}\,]$, assim como, por exemplo, $2 + \sqrt{-5}$ não divide ± 3 neste anel. Concluímos então que 9 e $6 + 3\sqrt{-5}$ não admitem máximo divisor comum em $\mathbb{Z}[\sqrt{-5}\,]$.

Capítulo 3

Anéis Fatoriais

Neste capítulo, estudamos os anéis principais e fatoriais. Seguem alguns resultados importantes, como por exemplo, todo anel principal é fatorial, mas não reciprocamente. Incluímos também um exemplo de um domínio de integridade que não é fatorial.

Em todo este capítulo, $\mathbb{A}$ é um domínio de integridade.

3.1 Anéis Principais

No Capítulo 1, vimos que um ideal $\mathbb{I}$ de um anel $\mathbb{A}$ é principal se $\mathbb{I}$ é gerado por um elemento deste anel, isto é, se existe $a \in \mathbb{A}$ tal que $\mathbb{I} = (a)$.

Definição 3.1. *Um anel $\mathbb{A}$ é dito principal se todos os ideais de $\mathbb{A}$ são principais.*

Teorema 3.2. *($\mathbb{Z}$ é um domínio principal). Todo ideal de $\mathbb{Z}$ é principal.*

Demonstração: Seja $\mathbb{I}$ um ideal de $\mathbb{Z}$. Se $\mathbb{I} = \{0\}$ então $\mathbb{I}$ é um ideal principal de $\mathbb{Z}$ gerado por 0.

Suponhamos que $\mathbb{I} \neq \{0\}$. Então existe $a \in \mathbb{I}$ tal que $a \neq 0$ daí, $-a \in \mathbb{I}$, isto é, $\mathbb{I}$ possui um inteiro positivo. Logo, podemos destacar em $\mathbb{I}$ um conjunto não-vazio de inteiros positivos. Pelo princípio da boa ordenação (veja [2], Capítulo II, § 2) existe $d \in \mathbb{I}$, tal que d é o menor inteiro positivo em $\mathbb{I}$. Mostramos que $\mathbb{I} = (d)$.

É claro que $(d) \subset \mathbb{I}$, pois $d \in \mathbb{I}$. Resta ver a outra inclusão.

Seja $x \in \mathbb{I}$. Então $|x| \in \mathbb{I}$, pois $\mathbb{I}$ é um ideal. Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$ tais que $|x| = qd + r$, onde $0 \leq r < d$. Portanto, $0 \leq |x| - qd < d$. Sendo que $|x|$ e $qd \in \mathbb{I}$, segue que $r \in \mathbb{I}$ e conseqüentemente $r = 0$, pois caso contrário teremos uma contradição com a minimalidade de d.

Logo, $|x| = qd \in (d)$, seguindo então que $\mathbb{I} = (d)$. □

Proposição 3.3. *Todo elemento irredutível de um anel principal $\mathbb{A}$ é primo.*

Demonstração: Seja p um elemento irredutível do anel $\mathbb{A}$. Assim, $p \neq 0$ e p não é invertível.

Suponhamos que $p|ab$, com $a, b \in \mathbb{A}$. Seja $\mathbb{I} = (p, a)$ o ideal de $\mathbb{A}$ gerado por p e a. Como $\mathbb{I}$ é principal, pois $\mathbb{A}$ é principal, então existe $d \in \mathbb{A}$ tal que $\mathbb{I} = (p, a) = (d)$. Assim, $p = dc$ para algum $c \in \mathbb{A}$ e sendo que p é irredutível segue que $d \in \mathbb{U}(\mathbb{A})$ ou $c \in \mathbb{U}(\mathbb{A})$.

Suponhamos que $d \in \mathbb{U}(\mathbb{A})$. Então existe $d' \in \mathbb{A}$ tal que $dd' = 1$. Como $d \in \mathbb{I}$, existem $x_0, y_0 \in \mathbb{A}$ tais que $d = px_0 + ay_0$. Logo, $1 = dd' = px_0d' + ay_0d'$. Multiplicando por b ambos os membros da igualdade temos que $b = (pb)x_0d' + (ab)y_0d'$. Como $p|pb$ e $p|ab$ segue que $p|(pb)x_0d' + (ab)y_0d'$, isto é, $p|b$.

Considerando o caso em que $c \in \mathbb{U}(\mathbb{A})$, segue facilmente que $p|a$.

Logo, p é primo. □

Exemplo 3.4. No anel $\mathbb{Z}$ dos números inteiros temos $\mathbb{U}(\mathbb{Z}) = \{\pm 1\}$. Logo, um número inteiro p, $p \neq 0$ e $p \neq \pm 1$, é irredutível se, e somente se, os únicos divisores de p são ± 1 e $\pm p$. Donde, p é irredutível se, e somente se, p é primo.

Proposição 3.5. *Um elemento $p \neq 0$ do anel principal $\mathbb{A}$ é irredutível (ou primo) se, e somente se, o ideal (p) é maximal.*

Demonstração: ($\Rightarrow$) Seja $\mathbb{I}$ um ideal de $\mathbb{A}$ tal que $(p) \subseteq \mathbb{I} \subseteq \mathbb{A}$. Temos que $\mathbb{I} = (a)$ para algum $a \in \mathbb{A}$, pois $\mathbb{A}$ é principal. Como $p \in \mathbb{I}$, segue que $p = aq$ para algum $q \in \mathbb{A}$. Sendo p irredutível, então $a \in \mathbb{U}(\mathbb{A})$ ou $q \in \mathbb{U}(\mathbb{A})$.

Se $a \in \mathbb{U}(\mathbb{A})$ então $\mathbb{I} = \mathbb{A}$. Considerando o caso em que $q \in \mathbb{U}(\mathbb{A})$ então $\mathbb{I} = (p)$. Logo, (p) é maximal.

($\Leftarrow$) Seja (p) um ideal maximal de $\mathbb{A}$. Então $(p) \neq \mathbb{A}$ e portanto, p não é invertível. Suponhamos $p = ab$, $a, b \in \mathbb{A}$. Claramente $(p) \subseteq (a)$. Logo, $(p) = (a)$ ou $(a) = \mathbb{A}$.

Se $(p) = (a)$ então existe $r \in \mathbb{A}$ tal que $a = pr$. Assim $p = prb$ e portanto, $rb = 1$, pois $\mathbb{A}$ é domínio de integridade e $p \neq 0$. Logo, $b \in \mathbb{U}(\mathbb{A})$. Se $(a) = \mathbb{A}$ então existe $s \in \mathbb{A}$ tal que $1 = as$ e claramente $a \in \mathbb{U}(\mathbb{A})$.

Logo, p é um elemento irredutível (ou primo) em $\mathbb{A}$. □

Lema 3.6. *Sejam $\mathbb{A}$ um anel principal e $\mathbb{I}_0 \subseteq \mathbb{I}_1 \subseteq \mathbb{I}_2 \subseteq \cdots$ uma sequência de ideais de $\mathbb{A}$. Então esta sequência é estacionária, ou seja, existe $r \in \mathbb{N}$ tal que $\mathbb{I}_r = \mathbb{I}_{r+1} = \cdots$.*

Demonstração: Consideramos $\mathbb{I} = \bigcup_{i \in \mathbb{N}} \mathbb{I}_i$ e como $\mathbb{I}_0 \subseteq \mathbb{I}_1 \subseteq \mathbb{I}_2 \subseteq \cdots$ temos que $\mathbb{I}$ é um ideal de $\mathbb{A}$. Sendo $\mathbb{A}$ um anel principal, segue que $\mathbb{I} = (d)$ para algum $d \in \mathbb{I}$. Logo, $d \in \mathbb{I}_r$ para algum $r \in \mathbb{N}$ e portanto $\mathbb{I} = (d) \subseteq \mathbb{I}_r \subseteq \mathbb{I}$, donde $\mathbb{I} = \mathbb{I}_r$. Evidentemente, $\mathbb{I}_r = \mathbb{I}_{r+1} = \cdots$. □

Lema 3.7. *Sejam $\mathbb{A}$ um anel principal e $a \in \mathbb{A}$ um elemento não-nulo e não invertível. Então a possui um divisor irredutível em $\mathbb{A}$.*

Demonstração: Seja $\mathbb{I}_0 = (a)$. Se $\mathbb{I}_0$ é maximal então, pela Proposição 3.5, a é irredutível.

Se $\mathbb{I}_0$ não é maximal então existe $\mathbb{I}_1$ um ideal de $\mathbb{A}$ tal que $\mathbb{I}_0 \subsetneq \mathbb{I}_1 \subsetneq \mathbb{A}$. Claramente, $\mathbb{I}_1 = (a_1)$ para algum $a_1 \in \mathbb{A}$, pois $\mathbb{A}$ é principal. Novamente, se $\mathbb{I}_1$ é maximal então a_1 é irredutível e como $a \in \mathbb{I}_1$, segue que $a_1 | a$.

Se $\mathbb{I}_1$ não é maximal, então existe um ideal $\mathbb{I}_2$ de $\mathbb{A}$ tal que $\mathbb{I}_0 \subsetneq \mathbb{I}_1 \subsetneq \mathbb{I}_2 \subsetneq \mathbb{A}$. Assim, sucessivamente, obtemos uma seqüência de ideais de $\mathbb{A}$ que pelo Lema 3.6 é estacionária. Portanto, existe $r \in \mathbb{N}$ tal que $\mathbb{I}_r = (a_r)$ é maximal e daí, a_r é irredutível. Como $\mathbb{I}_0 = (a) \subseteq \mathbb{I}_r = (a_r)$, vem que $a_r | a$ e segue o resultado. □

Teorema 3.8. *Seja $\mathbb{A}$ um anel principal. Então, para todo $a \in \mathbb{A}$, não-nulo e não invertível, existem $p_1, p_2, \cdots, p_n$ $(n \geq 1)$ irredutíveis tais que $a = p_1 p_2 \cdots p_n$. Além disso, se $a = q_1 q_2 \cdots q_s$, onde cada q_j é irredutível para $j = 1, 2, \cdots, s$, então $n = s$ e cada p_i é associado de algum q_j.*

Demonstração: Se a é irredutível então termina a demonstração. Suponhamos que a não seja irredutível. Pelo Lema 3.7, existe um elemento irredutível $p_1 \in \mathbb{A}$ tal que $a = p_1 a_1$ para algum $a_1 \in \mathbb{A}$. É claro que a_1 não é invertível, pois a não é irredutível.

Se a_1 é irredutível, termina a demonstração. Caso contrário, existe um elemento irredutível $p_2 \in \mathbb{A}$ tal que $a_1 = p_2 a_2$ para algum $a_2 \in \mathbb{A}$, não invertível. Então $a = p_1 p_2 a_2$.

Afirmamos que existe um índice $n \in \mathbb{N}$ tal que $a_n = p_n$ é irredutível. De fato, se tivéssemos uma seqüência infinita de elementos $a_1, a_2, \cdots$ não irredutíveis, teríamos então $\mathbb{I}_1 = (a_1) \subsetneq \mathbb{I}_2 = (a_2) \subsetneq \mathbb{I}_3 = (a_3) \subsetneq \cdots$ e isto contradiz o Lema 3.6.

Logo, $\exists\ n \in \mathbb{N}$ tal que $a = p_1 p_2 \cdots p_n$, onde cada p_i é irredutível para $i = 1, 2, \cdots, n$.

Agora, mostramos a unicidade desta decomposição. Suponhamos $p_1 \cdots p_n = q_1 q_2 \cdots q_s$ e isto implica que p_1 divide $q_1 \cdots q_s$. Pela Proposição 3.3, p_1 é primo e portanto divide um dos fatores, digamos $p_1 | q_1$. Logo, $q_1 = u_1 p_1$ onde $u_1 \in \mathbb{U}(\mathbb{A})$ e daí, $p_1 \sim q_1$.

Temos então que $p_1 p_2 \cdots p_n = u_1 p_1 q_2 \cdots q_s$ e por ser $\mathbb{A}$ domínio de integridade, segue que $p_2 \cdots p_n = u_1 q_2 \cdots q_s$. Repetindo o raciocínio, vem que $p_2 | q_2$ (reordenando os índices) e isto implica que $q_2 = u_2 p_2$, onde $u_2 \in \mathbb{U}(\mathbb{A})$ e daí, $p_2 \sim q_2$.

Assim, sucessivamente, resulta que $n = s$. De fato, sem perda de generalidade, suponhamos $s > n$. Então $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_n q_{n+1} \cdots q_s$ onde $q_i = u_i p_i$, $i = 1, 2, \cdots, n$ (por uma reordenação de índices). Logo, $u q_{n+1} q_{n+2} \cdots q_s = q_{n+1}(u q_{n+2} \cdots q_s) = 1$ onde $u = u_1 u_2 \cdots u_n$ e isto nos diz que q_{n+1} é invertível, absurdo pois q_{n+1} é irredutível. O mesmo absurdo é obtido se considerarmos $n > s$. Logo, $n = s$. □

3.2 Anéis Fatoriais

Definição 3.9. *Um domínio de integridade $\mathbb{A}$ é dito um anel fatorial se:*
(i) *Todo elemento $a \in \mathbb{A}$, não-nulo e não invertível, pode ser escrito como um produto de elementos irredutíveis de $\mathbb{A}$, isto é, $a = p_1 p_2 \cdots p_n$, onde $n \geq 1$ e os $p_i{}'s$ são irredutíveis;*
(ii) *Se $a = p_1 p_2 \cdots p_r$ e $a = q_1 q_2 \cdots q_s$, com p_i e q_j irredutíveis em $\mathbb{A}$, então $r = s$ e cada p_i é associado de algum q_j.*

Exemplo 3.10. Todo anel principal é fatorial, segue do Teorema 3.8.

Exemplo 3.11. Todo corpo é um anel fatorial. De fato, todos os seus elementos, exceto o zero, são invertíveis. Logo, não há elementos em $\mathbb{K}$ que contrariam a definição.

Exemplo 3.12. $\mathbb{Z}$ é um anel fatorial, pois $\mathbb{Z}$ é um anel principal (veja Teorema 3.2).

Se $\mathbb{A}$ é um anel fatorial, então na decomposição em fatores irredutíveis de um elemento $a \in \mathbb{A}$, não-nulo e não invertível, pode ocorrer que alguns pares de fatores sejam associados.

Podemos ter, por exemplo, dois fatores irredutíveis p e q distintos, porém associados. Logo, $q = up$ para $u \in \mathbb{U}(\mathbb{A})$ e daí $pq = up^2$. Repetindo esse raciocínio, a decomposição apresenta-se como $a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$, sempre que dois ou mais fatores irredutíveis forem associados, u é um produto de invertíveis e portanto invertível, $r \geq 1$, $\alpha_i^{'}s$ são inteiros positivos e entre estes $p_i^{'}s$ não há associados.

É sempre possível decompor dois elementos em fatores irredutíveis de um anel fatorial de maneira que em ambas tenhamos os mesmos fatores irredutíveis. Para isso, basta expressar em uma os elementos que não aparecem na outra (e vice-versa), escrevendo-os com expoente nulo. Assim, se a e b são dois elementos de $\mathbb{A}$ podemos escrevê-los da seguinte forma:

$$a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r} \quad e \quad b = vp_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r},$$

onde $\alpha_i, \beta_i \geq 0$, u e v são invertíveis.

Proposição 3.13. *Dois elementos quaisquer a e b, não simultaneamente nulos, de um anel fatorial $\mathbb{A}$ possuem máximo divisor comum.*

Demonstração: Se $a = 0$ então b é um máximo divisor comum de a e b, o mesmo para o caso $b = 0$.

Se $a \in \mathbb{U}(\mathbb{A})$ então $b = b1 = (ba^{'})a$, onde $a^{'}a = 1$ e a é um máximo divisor comum de a e b. Se $b \in \mathbb{U}(\mathbb{A})$ então, neste caso, b é um máximo divisor comum de a e b.

Caso contrário, escrevemos $a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ e $b = vp_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}$. Tomamos $d = p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_r^{\gamma_r}$, onde $\gamma_i = \text{mín}\{\alpha_i, \beta_i\}$. Afirmamos que d é um máximo divisor comum de a e b. De fato, $d|a$ e $d|b$, pois $\gamma_i \leq \alpha_i$ e $\gamma_i \leq \beta_i$.

Suponhamos $d' \in \mathbb{A}$ tal que $d'|a$ e $d'|b$. Então $d' = u' p_1^{\theta_1} p_2^{\theta_2} \cdots p_r^{\theta_r}$, onde $\theta_i \leq \alpha_i, \beta_i$ e $u' \in \mathbb{U}(\mathbb{A})$. Logo, $\theta_i \leq \text{mín}\{\alpha_i, \beta_i\} = \gamma_i$ e daí, $d'|d$. □

Proposição 3.14. *Seja $\mathbb{A}$ um anel fatorial. Então todo elemento irredutível de $\mathbb{A}$ é primo.*

Demonstração: Seja $p \in \mathbb{A}$ um elemento irredutível. Suponhamos que $p|ab$ para $a, b \in \mathbb{A}$. Logo, $ab = pq$ para algum $q \in \mathbb{A}$. Decompondo cada um dos fatores do primeiro membro da equação em fatores irredutíveis, segue que p é associado de um desses fatores, pois $\mathbb{A}$ é fatorial. Se esse for um fator de a, então $p|a$. Caso contrário, $p|b$. □

Proposição 3.15. *Se a e b são elementos não simultaneamente nulos de um anel fatorial e se d é um máximo divisor comum desses elementos no anel, então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.*

Demonstração: Sejam $a = up_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $b = vp_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$ e $d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$, onde $\gamma_i = \text{mín}\{\alpha_i, \beta_i\}$. Logo, os fatores de $\frac{a}{d}$ e $\frac{b}{d}$ são $p_i^{\alpha_i - \gamma_i}$ e $p_i^{\beta_i - \gamma_i}$, respectivamente.

Assim, $\alpha_i - \gamma_i = 0$ ou $\beta_i - \gamma_i = 0$, pois $\gamma_i = \text{mín}\{\alpha_i, \beta_i\}$, $i \in \{1, 2, \cdots, r\}$. Portanto, $\text{mín}\{\alpha_i - \gamma_i, \beta_i - \gamma_i\} = 0$ e como esse é o expoente de p_i do máximo divisor comum de $\frac{a}{d}$ e $\frac{b}{d}$, então $mdc(\frac{a}{d}, \frac{b}{d}) = 1$ seguindo que $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si. □

Proposição 3.16. *Sejam $\mathbb{A}$ um anel fatorial, a e b elementos de $\mathbb{A}$ que não são primos entre si. Então a e b têm um divisor comum irredutível.*

Demonstração: Seja $d \neq 0$ um máximo divisor comum de a e b em $\mathbb{A}$. Temos que d não é invertível, pois caso contrário $d \sim 1$ contrariando a hipótese de que $mdc(a, b) \neq 1$. Logo, d pode ser decomposto em fatores irredutíveis. Obviamente, qualquer um desses fatores divide a e b simultaneamente. □

Apresentamos um exemplo de um anel que não é fatorial e conseqüentemente não é um anel principal.

Exemplo 3.17. O anel $\mathbb{Z}[\sqrt{-6}\,]$ não é fatorial. De fato, $10 = 2 \cdot 5 = (2 + \sqrt{-6}\,)(2 - \sqrt{-6}\,)$. É fácil verificar que 2 e 5 são irredutíveis em $\mathbb{Z}[\sqrt{-6}\,]$. Mostramos que $2 \pm \sqrt{-6}$ também são irredutíveis. Antes lembramos que $\mathbb{U}(\mathbb{Z}[\sqrt{-6}\,]) = \{\pm 1\}$.

Suponhamos $2+\sqrt{-6}=\alpha\beta$, onde $\alpha=a+b\sqrt{-6}$ e $\beta=c+d\sqrt{-6}$ são elementos de $\mathbb{Z}[\sqrt{-6}\,]$. Logo, $10=N(\alpha)N(\beta)$. Temos as possibilidades:
(i) $N(\alpha)=1$ e $N(\beta)=10$ (e vice-versa). Neste caso, $a=\pm1$ e $b=0$ e $c=\pm2$ e $d=\pm1$, isto é, $\alpha=1$ e $\beta=2+\sqrt{-6}$ ou $\alpha=-1$ e $\beta=-2-\sqrt{-6}$. Logo, $\alpha\in\mathbb{U}(\mathbb{Z}[\sqrt{-6}\,])$.
(ii) $N(\alpha)=2$ e $N(\beta)=5$ (e vice-versa). Esta possibilidade claramente não ocorre, pois $a^2+6b^2=2$ e $c^2+6d^2=5$ não possuem solução em $\mathbb{Z}$.

Concluímos que $2+\sqrt{-6}$ é irredutível e de maneira análoga, $2-\sqrt{-6}$ também o é.

Mostramos que 2 e $2\pm\sqrt{-6}$ não são associados. Suponhamos que $2|2+\sqrt{-6}$. Então $2+\sqrt{-6}=2(a+b\sqrt{-6}\,)=2a+2b\sqrt{-6}$ e isto implica que $2b=1$, o que é um absurdo, pois $b\in\mathbb{Z}$.

Analogamente, $2\nmid 2-\sqrt{-6}$ em $\mathbb{Z}[\sqrt{-6}\,]$. Também, 5 e $2\pm\sqrt{-6}$ não são associados. Portanto, existem duas decomposições distintas para 10 em $\mathbb{Z}[\sqrt{-6}\,]$ mostrando que este anel não é fatorial.

Capítulo 4

Polinômios sobre um Anel Fatorial

Neste capítulo trabalhamos com anéis de polinômios (estes sobre anéis). Admitimos sabidas definições e algumas propriedades principais. Solicitamos consulta em ([1], Capítulo VI).

O principal resultado deste capítulo diz que se o anel $\mathbb{A}$ é fatorial então $\mathbb{A}[x]$ é também fatorial, isto é, o anel de polinômios cujos coeficientes estão em um anel fatorial é fatorial. Nosso objetivo é prová-lo, para isso apresentamos alguns lemas e definições.

Neste capítulo, $\mathbb{A}$ é um domínio de integridade.

Teorema 4.1. *Se $\mathbb{A}$ é um domínio de integridade, então $\mathbb{A}[x]$ também é um domínio de integridade.*

Demonstração: Sejam $f(x), g(x) \in \mathbb{A}[x]$ polinômios não-nulos. Para fixar idéias, suponhamos $f(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + a_mx^m$, onde $a_m \neq 0$ e $a_{m+j} = 0$, $\forall\ j \in \mathbb{N}^*$ e $g(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} + b_nx^n$, onde $b_n \neq 0$ e $b_{n+j} = 0$, $\forall\ j \in \mathbb{N}^*$. Então $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n}$ e como $c_{m+n} = a_0b_{m+n} + a_1b_{m+n-1} + \cdots + a_mb_n + a_{m+1}b_{n-1} + \cdots + a_{m+n}b_0 = a_mb_n \neq 0$, pois a_m e b_n são elementos não-nulos de $\mathbb{A}$ que é um domínio de integridade, segue que $f(x)g(x) \neq 0$ e isto mostra que $\mathbb{A}[x]$ é um domínio de integridade. □

Definição 4.2. *Um polinômio $f(x) = a_0+a_1x+\cdots+a_mx^m \in \mathbb{A}[x]$ é primitivo*

se $f(x)$ não é um polinômio constante e se os seus coeficientes são primos entre si, isto é, admitem a unidade de $\mathbb{A}$ como máximo divisor comum.

Exemplo 4.3. O polinômio $f(x) = x + 3x^2 - 4x^4 \in \mathbb{Z}[x]$ é primitivo, pois $mdc(-4, 1, 3) = 1$.

Exemplo 4.4. O polinômio $g(x) = 8x + 12x^5 \in \mathbb{Z}[x]$ não é primitivo, pois $mdc(8, 12) = 4$.

Exemplo 4.5. $h(x) = \frac{3}{2} - 3x + 5x^3 \in \mathbb{R}[x]$ é primitivo, pois em $\mathbb{R}$ todos os elementos não-nulos são associados.

Observação: Seja $\mathbb{A}$ um domínio de integridade. Então $\mathbb{U}(\mathbb{A}) = \mathbb{U}(\mathbb{A}[x])$.

De fato, temos que claramente $\mathbb{U}(\mathbb{A}) \subseteq \mathbb{U}(\mathbb{A}[x])$, pois $\mathbb{A} \subseteq \mathbb{A}[x]$. Suponhamos $f(x) \in \mathbb{U}(\mathbb{A}[x])$. Então existe $g(x) \in \mathbb{A}[x]$ tal que $f(x)g(x) = 1$. Logo, $\partial f(x) = \partial g(x) = 0$ e portanto $f(x) = a \neq 0$ e $g(x) = b \neq 0$, onde $a, b \in \mathbb{A}$. Segue então que $ab = 1$, isto é, $f(x) = a \in \mathbb{U}(\mathbb{A})$. Assim, $\mathbb{U}(\mathbb{A}) = \mathbb{U}(\mathbb{A}[x])$.

Exemplo 4.6. Consideramos o anel $\mathbb{Z}_9$ que não é um domínio de integridade. Os polinômios $\bar{1}+\bar{3}x^2$ e $\bar{1}+\bar{6}x^2$ estão em $\mathbb{U}(\mathbb{Z}_9[x])$, pois $(\bar{1}+\bar{3}x^2)(\bar{1}+\bar{6}x^2) = \bar{1}$.

Este exemplo mostra que se $\mathbb{A}$ não é um domínio de integridade então $\mathbb{U}(\mathbb{A}[x])$ pode ser diferente de $\mathbb{U}(\mathbb{A})$.

Proposição 4.7. *Se $\mathbb{A}$ é fatorial e $f(x) \in \mathbb{A}[x]$ é irredutível e não constante, então $f(x)$ é primitivo.*

Demonstração: Suponhamos que $f(x)$ não seja primitivo. Então $f(x) = df^*(x)$, onde d é um máximo divisor comum dos coeficientes de $f(x)$ (isto é possível, pois $\mathbb{A}$ é fatorial) e claramente d não é invertível, pois caso contrário d e 1 são associados e isto implica que 1 é um máximo divisor comum dos coeficientes de $f(x)$, o que é absurdo pois estamos supondo que $f(x)$ não é primitivo. Por outro lado, $f^*(x)$ também não é invertível uma vez que $\partial f^*(x) = \partial f(x) \neq 0$ e $\mathbb{U}(\mathbb{A}[x]) = \mathbb{U}(\mathbb{A})$.

Chegamos a um absurdo, pois neste caso, $f(x)$ não é um polinômio irredutível em $\mathbb{A}[x]$ e isto contraria a hipótese. □

Exemplo 4.8. Um polinômio primitivo pode não ser irredutível. De fato, o polinômio $f(x) = -3 - x + 6x^2 + 2x^3$ é claramente primitivo em $\mathbb{Z}[x]$, mas

$f(x) = (x+3)(2x^2-1)$. Logo, $f(x)$ não é irredutível, pois $\mathbb{U}(\mathbb{Z}[x]) = \mathbb{U}(\mathbb{Z}) = \{\pm 1\}$.

Lema 4.9. *Seja $f(x) \in \mathbb{A}[x]$ um polinômio não constante. Então existem um polinômio primitivo $f^*(x) \in \mathbb{A}[x]$ e um elemento $d \in \mathbb{A}$ tais que $f(x) = df^*(x)$. Além disso, se $f(x) = d_1 f_1^*(x)$, com $d_1 \in \mathbb{A}$ e $f_1^*(x)$ primitivo em $\mathbb{A}[x]$, então $d \sim d_1$ e $f^*(x) \sim f_1^*(x)$.*

Demonstração: Suponhamos $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e seja $d = mdc(a_0, a_1, \cdots, a_n)$. Chamando $f^*(x) = \frac{a_0}{d} + \frac{a_1}{d}x + \cdots + \frac{a_n}{d}x^n$ temos que $f(x) = df^*(x) = d(\frac{a_0}{d} + \frac{a_1}{d}x + \cdots + \frac{a_n}{d}x^n)$. Pela Proposição 3.15, f^* é primitivo.

Suponhamos agora que $f(x) = df^*(x) = d_1 f_1^*(x)$ com $d_1 \in \mathbb{A}$ e $f_1^*(x)$ primitivo. Temos que $d_1 | a_i$ para todo $i \in \{0, 1, 2, \cdots, n\}$. Logo $d_1 | d$ e portanto, $d = d_1 c$ para algum $c \in \mathbb{A}$.

Assim, $d_1 f_1^*(x) = df^*(x) = d_1 c f^*(x)$ e isto implica que $cf^*(x) = f_1^*(x)$. Portanto, c divide todos os coeficientes de $f_1^*(x)$. Sendo $f_1^*(x)$ primitivo, temos que $c|1$, ou seja, $c \in \mathbb{U}(\mathbb{A})$. Como $d = d_1 c$ e $cf^*(x) = f_1^*(x)$ segue que $d_1 \sim d$ e $f^*(x) \sim f_1^*(x)$. □

Lema 4.10. *O produto de dois polinômios primitivos sobre um anel fatorial é um polinômio primitivo.*

Demonstração: Sejam $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$ e $g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$ polinômios primitivos em $\mathbb{A}[x]$ de graus m e n respectivamente. Suponhamos que $f(x)g(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{m+n}x^{m+n}$ não seja primitivo, onde $c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_1b_{i-1} + a_0b_i$. Então, pela Proposição 3.16 existe um elemento irredutível $p \in \mathbb{A}$ tal que $p | c_k$ para $k = 0, 1, \cdots, m+n$.

Sendo p irredutível e como $p | a_0b_0$ (pois $c_0 = a_0b_0$) segue que $p | a_0$ ou $p | b_0$. Vamos supor que $p | a_0$. Então existe r, $0 < r \leq m$ tal que $p | a_1$, $\cdots$, $p | a_{r-1}$ e $p \nmid a_r$. Como $c_r = a_0b_r + a_1b_{r-1} + \cdots + a_rb_0$ e sendo que $p | a_i$ para $i \in \{0, 1, \cdots, r-1\}$, segue que $p | a_rb_0$ e isto implica que $p | b_0$, pois p é primo e $p \nmid a_r$.

Assim, existe s, $0 < s \leq n$ tal que $p | b_i$ para $i \in \{1, 2, \cdots, s-1\}$ e $p \nmid b_s$. Sabendo que $c_{r+s} = a_0b_{r+s} + a_1b_{(r+s)-1} + \cdots + a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} +$

$\cdots + a_{r+s}b_0$ isto implica que $p|a_r b_s$, pois $p|c_{r+s}$, $p|a_i$ para $i = 0, 1, \cdots, r-1$ e $p|b_i$ para $i = 1, 2, \cdots, s-1$ e isto é um absurdo, pois então $p|a_r$ ou $p|b_s$. □

Definimos abaixo o corpo de frações de um domínio de integridade que é usado nos dois lemas posteriores. Na verdade, existe uma construção deste corpo usando relação de equivalência. No entanto, não a apresentamos aqui, para maiores detalhes (veja [1], Capítulo V, V-3 10 e [2], Capítulo III, § 5). Chamamos $\mathbb{A}^* = \mathbb{A} - \{0\}$.

Definição 4.11. *Dado um domínio de integridade* $\mathbb{A}$*, o conjunto* $\mathbb{K} = \{\frac{a}{b} : a \in \mathbb{A} \text{ e } b \in \mathbb{A}^*\}$ *possui uma estrutura de corpo, o qual é dito corpo de frações do domínio* $\mathbb{A}$*.*

Lema 4.12. *Seja* $\mathbb{K}$ *o corpo de frações de um anel fatorial* $\mathbb{A}$*. Se* $F(x) \in \mathbb{K}[x]$ *não é constante, então existem* $a, b \in \mathbb{A}^*$ *e um polinômio primitivo* $f^*(x) \in \mathbb{A}[x]$ *tais que* $F(x) = \frac{a}{b} f^*(x)$*. Além disso, se* $F(x) = \frac{a_1}{b_1} f_1^*(x)$*, com* $a_1, b_1 \in \mathbb{A}^*$ *e* $f_1^*(x) \in \mathbb{A}[x]$ *também primitivo, então* $ab_1 \sim a_1 b$ *e* $f^*(x) \sim f_1^*(x)$*.*

Demonstração: Sendo que $F(x) \in \mathbb{K}[x]$, podemos escrevê-lo como $F(x) = \frac{c_0}{d_0} + \frac{c_1}{d_1}x + \frac{c_2}{d_2}x^2 + \cdots + \frac{c_m}{d_m}x^m$ e tomando $d_0 d_1 \cdots d_m = b \neq 0$, pois $\mathbb{A}$ é um domínio de integridade, segue que $F(x) = \frac{1}{b} f(x)$, onde $f(x) = c_0 d_1 \cdots d_m + c_1 d_0 d_2 \cdots d_m x + \cdots + c_m d_0 \cdots d_{m-1} x^m \in \mathbb{A}[x]$. Pelo Lema 4.9, $f(x) = a f^*(x)$ com $f^*(x)$ primitivo em $\mathbb{A}[x]$ e $a \in \mathbb{A}^*$. Logo, $F(x) = \frac{a}{b} f^*(x)$.

Por outro lado, se $F(x) = \frac{a}{b} f^*(x) = \frac{a_1}{b_1} f_1^*(x)$ então $ab_1 f^*(x) = a_1 b f_1^*(x)$ e pelo Lema 4.9, vem que $ab_1 \sim a_1 b$ e $f^*(x) \sim f_1^*(x)$. □

Lema 4.13. *Seja* $\mathbb{K}$ *o corpo de frações do anel fatorial* $\mathbb{A}$*. Se o polinômio* $f(x) \in \mathbb{A}[x]$ *é irredutível sobre* $\mathbb{A}$*, então* $f(x)$ *é também irredutível sobre* $\mathbb{K}$*.*

Demonstração: Suponhamos por absurdo que $f(x)$ não seja irredutível sobre $\mathbb{K}$. Então existem $G(x), H(x) \in \mathbb{K}[x]$, não constantes, tais que $f(x) = G(x)H(x)$. Pelo Lema 4.12 segue que $G(x) = \frac{a}{b} g^*(x)$ e $H(x) = \frac{c}{d} h^*(x)$, com $a, b, c, d \in \mathbb{A}^*$ e $g^*(x), h^*(x)$ polinômios primitivos em $\mathbb{A}[x]$.

Logo, $f(x) = \frac{ac}{bd} g^*(x)h^*(x)$ e portanto, $bdf(x) = acg^*(x)h^*(x)$. Pelo Lema 4.10, $g^*(x)h^*(x)$ é primitivo em $\mathbb{A}[x]$. Como ac e bd são associados, existe $u \in \mathbb{U}(\mathbb{A})$ tal que $ac = u(bd)$. Assim, $f(x) = ug^*(x)h^*(x)$.

Como $\partial(ug^*(x)) = \partial G(x) \geq 1$ e $\partial h^*(x) = \partial H(x) \geq 1$, segue que $f(x)$ não é irredutível em $\mathbb{A}[x]$ e isto contradiz a hipótese. Logo, $f(x)$ é irredutível sobre $\mathbb{K}$. □

Lema 4.14. *Seja $\mathbb{A}$ um anel fatorial. Então todo polinômio irredutível $f(x) \in \mathbb{A}[x]$ é também primo.*

Demonstração: Suponhamos $f(x)$ um polinômio constante. Então $f(x) \in \mathbb{A}$ e por hipótese $f(x)$ é irredutível em $\mathbb{A}[x]$ logo, irredutível em $\mathbb{A}$. Pela Proposição 3.14, $f(x)$ é primo em $\mathbb{A}$, pois $\mathbb{A}$ é um anel fatorial. Portanto, $f(x)$ é primo em $\mathbb{A}[x]$.

Suponhamos agora que $\partial f(x) \geq 1$. Sejam $g(x), h(x) \in \mathbb{A}[x]$ tais que $f(x)$ divide $g(x)h(x)$ em $\mathbb{A}[x]$. É claro que $f(x)$ divide $g(x)h(x)$ em $\mathbb{K}[x]$, onde $\mathbb{K}$ é o corpo de frações de $\mathbb{A}$. Como $\mathbb{K}[x]$ é um anel principal (veja [2], Capítulo IV, Teorema 2) e $f(x)$ é primo em $\mathbb{K}[x]$, então $f(x)|g(x)$ ou $f(x)|h(x)$ em $\mathbb{K}[x]$.

Considerando a primeira possibilidade temos que existe $H(x) \in \mathbb{K}[x]$ tal que $g(x) = H(x)f(x)$.

Pelo Lema 4.9 temos que $g(x) = dg^*(x)$ para convenientes $d \in \mathbb{A}$ e $g^*(x)$ primitivo em $\mathbb{A}[x]$.

Pelo Lema 4.12 temos que $H(x) = \frac{a}{b}h^*(x)$, com $a, b \in \mathbb{A}^*$ e $h^*(x) \in \mathbb{A}[x]$.

Logo, $g(x) = H(x)f(x)$ implica em $dg^*(x) = \frac{a}{b}h^*(x)f(x)$. Do Lema 4.9 segue que $d \sim \frac{a}{b}$ e assim existe $u \in \mathbb{U}(\mathbb{A})$ tal que $\frac{a}{b} = ud$.

Segue que $g(x) = dg^*(x) = (udh^*(x))f(x)$ e portanto, $f(x)$ divide $g(x)$ em $\mathbb{A}[x]$, pois $udh^*(x) \in \mathbb{A}[x]$. □

O resultado a seguir é o mais importante deste capítulo.

Teorema 4.15. *Se $\mathbb{A}$ é um anel fatorial, então $\mathbb{A}[x]$ é fatorial.*

Demonstração: Seja $f(x) \in \mathbb{A}[x]$, $f(x) \neq 0$ e $f(x)$ não invertível.

Se $\partial f(x) = 0$ então $f(x) \in \mathbb{A}$ e como $\mathbb{A}$ é um anel fatorial segue que $f(x)$ pode ser decomposto como um produto de elementos irredutíveis em $\mathbb{A}$ e portanto irredutíveis em $\mathbb{A}[x]$.

Suponhamos que $\partial f(x) = n \geq 1$ e adimitimos por hipótese de indução que a decomposição é válida para todo polinômio de grau r, onde $0 \leq r < n$. Pelo

Lema 4.9 $f(x) = df^*(x)$ para convenientes $d \in \mathbb{A}$ e um polinômio primitivo $f^*(x) \in \mathbb{A}[x]$.

Se $f^*(x)$ é irredutível então basta decompor d em fatores irredutíveis em $\mathbb{A}$, o que é possível pois $\mathbb{A}$ é um anel fatorial. Caso $f^*(x)$ não seja irredutível, então existem $g(x), h(x) \in \mathbb{A}[x]$ tais que $f^*(x) = g(x)h(x)$, com $1 \leq \partial g(x), \partial h(x) < \partial f(x) = \partial f^*(x)$.

Aplicando a hipótese de indução para os polinômios $g(x)$ e $h(x)$ segue o resultado, pois teremos uma decomposição de d e de $f^*(x)$ em fatores irredutíveis em $\mathbb{A}[x]$.

Mostramos a unicidade da decomposição acima.

Sejam $g_1(x)g_2(x)\cdots g_r(x)$ e $h_1(x)h_2(x)\cdots h_s(x)$ duas decomposições em fatores irredutíveis de $f(x)$ em $\mathbb{A}[x]$.

Então $g_1(x)g_2(x)\cdots g_r(x) = h_1(x)h_2(x)\cdots h_s(x)$ e assim, $g_1(x)$ divide $h_1(x)h_2(x)\cdots h_s(x)$. Pelo Lema 4.14, $g_1(x)$ é primo e portanto divide um dos polinômios $h_i(x)$ em $\mathbb{A}[x]$ para $i \in \{1, 2, \cdots, s\}$. Suponhamos que $g_1(x)|h_1(x)$. Como $g_1(x)$ é irredutível (portanto não invertível) segue que existe $u_1(x) \in \mathbb{U}(\mathbb{A}[x])$ tal que $h_1(x) = u_1(x)q_1(x)$. Donde $g_1(x) \sim h_1(x)$.

Segue que $g_1(x)g_2(x)\cdots g_r(x) = u_1(x)g_1(x)h_2(x)\cdots h_s(x)$ e por ser $\mathbb{A}[x]$ um domínio de integridade $g_2(x)\cdots g_r(x) = u_1(x)h_2(x)\cdots h_s(x)$.

Usando o mesmo raciocínio acima (e reordenando os índices) temos que $g_2(x)|h_2(x)$ e portanto, $g_2(x) = u_2(x)h_2(x)$ para algum $u_2(x) \in \mathbb{U}(\mathbb{A}[x])$. Donde $g_2(x) \sim h_2(x)$.

Assim, sucessivamente, segue que $r = s$.

De fato, supondo $s > r$ segue que $g_1(x)g_2(x)\cdots g_r(x) = h_1(x)h_2(x)\cdots h_r(x)h_{r+1}(x)\cdots h_s(x)$ onde $h_j(x) = u_i(x)g_j(x), j \in \{1, 2, \cdots, r\}$.

Logo, $u(x)h_{r+1}(x)h_{r+2}(x)\cdots h_s(x) = h_{r+1}(x)(u(x)h_{r+2}(x)\cdots h_s(x))$ onde $u(x) = u_1(x)u_2(x)\cdots u_r(x)$ e isto implica que $h_{r+1}(x)$ é invertível em $\mathbb{A}[x]$, o que é um absurdo, pois o mesmo é irredutível em $\mathbb{A}[x]$. Se $r > s$ temos a mesma contradição. Portanto, $r = s$. □

O resultado anterior pode ser estendido:

Corolário 4.16. *Sejam $\mathbb{A}$ um anel fatorial e $\mathbb{A}[x_1, x_2, \cdots, x_n]$ o anel de polinômios nas indeterminadas $x_1, x_2, \cdots, x_n$ com coeficientes em $\mathbb{A}$. Então*

$\mathbb{A}[x_1, x_2, \cdots, x_n]$ *é um anel fatorial.*

Na Seção 3.2 vimos que todo anel principal é fatorial. Agora apresentamos dois exemplos que mostram que a recíproca deste resultado não vale.

Exemplo 4.17. Sendo $\mathbb{Z}$ um anel fatorial, então pelo Teorema 4.15 $\mathbb{Z}[x]$ também o é. Mostramos que $\mathbb{Z}[x]$ não é principal.

De fato, consideramos $\mathbb{I} = (2, x) = \{2p(x) + xq(x) : p(x), q(x) \in \mathbb{Z}[x]\}$. Suponhamos que $\mathbb{I}$ seja principal. Então existe $d(x) \in \mathbb{Z}[x]$ tal que $\mathbb{I} = d(x)\mathbb{Z}[x]$ e isto nos diz que $d(x)\mathbb{Z}[x] = 2\mathbb{Z}[x] + x\mathbb{Z}[x]$.

Temos que $x \in d(x)\mathbb{Z}[x]$. Logo, $x = d(x)q_1(x)$ para algum $q_1(x) \in \mathbb{Z}[x]$ e daí, $d(x)|x$. Analogamente, $d(x)|2$.

Obviamente, se $d_1(x)|x$ e $d_1(x)|2$ então $d_1(x)|d(x)$. Logo, $d(x)$ é um máximo divisor comum de 2 e x em $\mathbb{Z}[x]$. Temos que $d(x) = \pm 1$ ou $d(x) = \pm 2$, pois $d(x)|2$.

Suponhamos $d(x) = 2$. Então $x = 2q_1(x)$. Portanto, $\partial q_1(x) = 1$, isto é, $q_1(x) = a_0 + a_1 x$, com $a_0, a_1 \in \mathbb{Z}$. Donde, $x = 2a_0 + 2a_1 x$ e isto é um absurdo, pois $a_1 = \frac{1}{2}$ não pertence a $\mathbb{Z}$. Chegamos ao mesmo absurdo supondo $d(x) = -2$.

Logo, $d(x) = \pm 1$. Tomando $d(x) = 1$, existem $f_1(x), f_2(x) \in \mathbb{Z}[x]$ tais que $1 = 2f_1(x) + xf_2(x)$ e isto é um absurdo, pois o termo constante do segundo membro da igualdade é sempre par. O mesmo absurdo é obtido no caso em que $d(x) = -1$.

Portanto, $\mathbb{I}$ não é um ideal principal.

Exemplo 4.18. Seja $\mathbb{K}$ um corpo. Então $\mathbb{K}[x, y]$ é um anel fatorial, mas não é principal.

Consideramos o ideal gerado por x e y, isto é, $\mathbb{I} = (x, y) = \{xf(x, y) + yg(x, y) : f(x, y), g(x, y) \in \mathbb{K}[x, y]\}$. Suponhamos que $\mathbb{I}$ seja principal, então existe $d(x, y) \in \mathbb{K}[x, y]$ tal que $\mathbb{I} = d(x, y)\mathbb{K}[x, y]$. Portanto, $d(x, y)\mathbb{K}[x, y] = (x, y)$.

Temos que $x \in d(x, y)\mathbb{K}[x, y]$ então existe $f_1(x, y) \in \mathbb{K}[x, y]$ tal que $x = d(x, y)f_1(x, y)$. Logo $d(x, y)|x$. Analogamente, temos que $d(x, y)|y$ e portanto $y = d(x, y)|f_2(x, y)$. Além disso, se $d_1(x, y)|x$ e $d_1(x, y)|y$ então é claro que $d_1(x, y)$ divide $d(x, y)$. Logo, $d(x, y)$ é um máximo divisor comum de x e y em $\mathbb{K}[x, y]$.

Como $x = d(x,y)f_1(x,y)$, segue que $d(x,y) = h(x)$ e $f_1(x,y) = c \in \mathbb{K}$ ou $d(x,y) = c^{'} \in \mathbb{K}$ e $f_1(x,y) = h_1(x)$.

Na primeira possibilidade, $d(x,y) = ax$, $a \in \mathbb{K} - \{0\}$. Mas esta possibilidade não ocorre, pois ax não divide y em $\mathbb{K}[x,y]$.

Logo, $d(x,y) = c^{'} = xr_1(x,y) + yr_2(x,y)$ para $r_1(x,y), r_2(x,y) \in \mathbb{K}[x,y]$ e isto é um absurdo, pois o segundo membro da equação não é um polinômio constante.

Conclusão

Este trabalho possibilitou a prática constante da pesquisa, o aprimoramento de alguns conceitos vistos no curso e o contato com outros assuntos que deram continuidade ao nosso aperfeiçoamento.

O estudo dos anéis, do modo como abordamos, ampliou nosso conhecimento no sentido que trabalhamos também com anéis não-comutativos e portanto, outros conceitos surgiram como ideais à esquerda e à direita. Destacamos também outros tipos de anéis (comutativos) que não foram vistos durante o curso como os anéis quadráticos, os anéis principais e os anéis fatoriais.

A busca de exemplos e contra-exemplos, resultados que valiam em um anel e que não valiam em outros, contribuíram em muito para o modo de pensarmos matemática, enriquecendo a nossa formação.

Por isso, consideramos muito proveitoso a realização deste trabalho.

Finalmente, esperamos que este trabalho possa ser útil a outras pessoas como um material de estudo e/ou consulta.

Referências Bibliográficas

[1] Domingues, H.H. e Iezzi, G., *"Álgebra Moderna"*, Atual Editora, 4ª edição reformulada, São Paulo (2003).

[2] Gonçalves, A., *"Introdução à Álgebra"*, Projeto Euclides, IMPA, 5ª edição, Rio de Janeiro (2001).

[3] Herstein, I.N., *"Topics in Algebra"*, John Wiley & Sons, Inc., Second Edition, New York (1975).

[4] Lam, T.Y., *"A First Course in Noncommutative Rings"*, Graduate Texts in Mathematics, Springer-Verlag, New York (1991).

[5] Monteiro, J., *"Elementos de Álgebra"*, Ao Livro Técnico S.A., Rio de Janeiro (1969).

[6] Boyer, C.B., *"História da Matemática"*, Editora Edgard Blücher LTDA, 2ª Edição, São Paulo (1996).